Informacijska sigurnost u poslovanju

Profozić, Mario

Mario Profozić

INFORMACIJSKA SIGURNOST U POSLOVANJU

ZAVRŠNI RAD

Veleučilište u Karlovcu
Poslovni odjel
Stručni specijalistički studij Poslovno upravljanje

Kolegij: Informacijski sustavi
Mentorica: izv.prof.dr.sc. Ljerka Luić, prof.v.š.
Matični broj studenta: 0619414020

Karlovac, 2018.

VELEUČILIŠTE U KARLOVCU
POSLOVNI ODJEL
STRUČNI SPECIJALISTIČKI DIPLOMSKI STUDIJ
POSLOVNO UPRAVLJANJE

Mario Profozić

INFORMACIJSKA SIGURNOST U POSLOVANJU

ZAVRŠNI RAD

Karlovac, travanj 2018.

SADRŽAJ

SAŽETAK

INFORMACIJSKA SIGURNOST U POSLOVANJU

U ovom završnom radu predstavljen je opći dio informacijske sigurnosti u poslovanju organizacije. Glavni cilj ovog rada je pokazati čvrstu vezu između poslovanja organizacije i informacijske sigurnosti. Naslovna tema izabrana je iz razloga što se u svijetu stalno pojavljuju novi načini ugrožavanja informacijskih sustava od strane raznih kriminalnih skupina koje se bave kibernetskim kriminalom. Također postoje osobe odnosno skupine osoba koje se bave raznim oblicima poslovne špijunaže te kao takvi mogu pričiniti veliku štetu napadnutom informacijskom sustavu u organizaciji (poduzeću, državnoj upravi, banci itd.). Obzirom na sve navedeno, važno je među zaposlenicima probuditi i širiti svijest o informacijskoj sigurnosti te svakodnevno se obrazovati o novim dostigućima na polju informacijske sigurnosti. Norme iz serije ISO 27000 predstavljaju odgovor na izazov provođenja mjera informacijske sigurnosti u organizaciji.

Ključne riječi: Informacijski sustav, informacijska tehnologija, informacijska sigurnost, norma ISO 27000.

SUMMARY

INFORMATION SECURITY IN BUSINESS

This master's thesis presents the information security in the organization's business. The main purpose of this paper is to show a strong link between organization's business and information security. The theme was chosen because of new ways of endangering information systems in the world by various criminal groups dealing with cybercrime. There are also persons or groups of people involved in various forms of business espionage and as such can pose a great deal of damage to the attacked information system in the organization (enterprise, state administration, bank, etc.). Given all the above, it is important for employees to wake and spread awareness of information security and to educate themselves on new information security attainments on a daily basis. Standards from the ISO 27000 series represent an answer to the challenge of

implementing information security measures in the organization.

Key words: Information system, information technology, information security, ISO 27000 standard.

1. UVOD

1.1. Predmet i cilj rada

Predmet rada je informacijska sigurnost u poslovanju. Cilj rada je teoretski prikazati značajke informacijskih sustava i informacijske sigurnosti te povezanosti istih u poslovnim organizacijama te prezentacija teoretskih spoznaja na aplikativnom primjeru.

1.2. Izvori podataka i metode prikupljanja

Pri izradi završnog rada korištena je znanstvena i stručna literatura iz područja menadžmenta, i informacijskih tehnologija s posebnim interesom u području informacijske sigurnosti. Pri obradi teme, korišteni su sekundarni podaci, sa službenih internet stranica na kojima su objavljeni tekstovi ili radovi koji se odnose na tematsko područje ovog završnog rada. U radu su korištene metode deskriptivne analize (pri raščlanjivanju i opisu elemenata cjelina koje su obrađivane u ovom radu s ciljem utvrđivanja elemenata, sadržaja i sastavnica promatrane cjeline kao i odnosa u cjelini) i sinteze (pri sjedinjavanju jednostavnih misaonih tvorevina u složenije povezujući elemente, procese, pojave i odnose u cjelinu), induktivna i deduktivna metoda (u svrhu prezentiranja uopćenih zakonitosti i smanjenja apstrakcija) te metoda kompilacije (pri citiranju i grafičkim prikazima koji su preuzeti iz korištene literature).

1.3. Sadržaj i struktura rada

Ovaj završni rad sastoji se od četiri cjeline (poglavlja).
U prvom poglavlju objašnjen je pojam i elementi informacijskog sustava..
Drugo poglavlje se bavi informacijskom tehnologijom u poslovanju. Razlog obrade ovog poglavlja je zato što je u današnje vrijeme gotovo svaki proces u organizaciji potpomognut suvremenom informacijsko – komunikacijskom tehnologijom (ICT). Kao primjer ove teze je obično izdavanje računa za učinjenu uslugu ili isporučenu robu. Postoji klasični način izdavanja računa (račun izlazi iz printera umreženog računala) te drugi načini izdavanja računa bez umreženog računala, to su npr. blokovi koji se mogu kupiti u prodavaonicama Narodnih novina (račun, uplatnica, izdatnica itd.), ali na kraju se ako ništa drugo zbirne vrijednosti koje su na tim blokovima evidentirane moraju unesti negdje u sustav, dakle opet postoji dokaz da je ICT tehnologija neizbježna u poslovanju.
Treće poglavlje bavi se informacijskom sigurnosti. Mnogi, pa čak i poslovni ljudi zanemaruju informacijsku sigurnost. Razlog tomu je neznanje i nemar, no kad se dogodi šteta prouzrokovana djelovanjem osoba koje napadu informacijski sustav onda ljudi počinju shvaćati ozbiljnost problema koji je nastao.
Četvrto poglavlje odnosi se na norme iz serije ISO 27000. Prvo su ukratko objašnjene pojedine norme iz navedene serije. Zatim je detaljnije objašnjena norma ISO 27001. Navedena serija normi (ISO 27000) predstavlja kvalitetan odgovor na potencijalne ugoroze sigurnosti informacijskih sustava bilo koje organizacije, te sponu između operativnog menadžmenta i informacijske sigurnosti, tj. na što sve operatvni menadžeri moraju obratiti pažnju prilikom svakodnevnog obavljanja posla. Ovo poglavlje završava alikativnim primjerom, gdje je prikazano uvođenje norme ISO 27001 u organizaciju.

1.4. Hipoteza rada

Hipoteza rada sastoji se u tvrdnji da postoji univerzalni međunarodni standard odnosno norma po kojoj se može implementirati i certificirati sigurnost informacijskog sustava, a time i informacijska sigurnost u poslovanju.

2. INFORMACIJSKI SUSTAVI

U ovom poglavlju prezentirati će se pojam, elementi, funkcija te razvoj i životni ciklus informacijskog sustava.

2.1. Pojam informacijskog sustava

Informacija je resurs za rukovođenje, poput kapitala i rada, te predstavlja jednu od najznačajnijih upotreba informacijske tehnologije kao konkurentskog oružja. Kao resurs ima specifična obilježja jer za razliku od materije i energije ne troši se korištenjem, niti smanjuje raspodjelom. Ona se danas nalazi u središtu poslovanja i predstavlja njen centralni faktor. Dominacija informacijske funkcije ukazuje s jedne strane na potrebu informatizacije poslovanja unutar poslovnog sustava, a s druge strane na efikasno povezivanje s izvorima informacija iz njene okoline što tom okruženju osigurava uspješno poslovanje i izglednu budućnost. Jedino oni poslovni sustavi koji polažu dovoljno pažnje razvoju informacijskog sustava mogu se nositi sa složenim uvjetima svjetskog tržišta i konkurencije. Informacijski sustav poslovnog sustava izuzetno je značajan za njegovu opstojnost i poslovanje, stoga je njegovo strateško planiranje jednako važno koliko i strateško planiranje poslovnog sustava. Koji je u osnovi, temeljni cilj informacijskog sustava? Cilj je informacijskog sustava dostaviti pravu informaciju na pravo mjesto, u pravo vrijeme i uz minimalne troškove. Ali kako taj cilj ostvariti u praksi? Zasigurno ne tako lako. Osnovne zadaće informacijskog sustava su: prikupljanje, razvrstavanje, obrada, čuvanje, oblikovanje i raspoređivanje informacija na sve razine objektnog sustava, odnosno korisnicima.[1]

Informacijski sustav je skup dobro definiranih pravila, običaja i postupaka pomoću kojih ljudi, oprema ili jedno i drugo, rade na određenom inputu sa svrhom da dobiju informacije koje će zadovoljiti potrebe određenih pojedinaca u određenoj poslovnoj situaciji.[2]

[1] Luić Lj.: Informacijski sustavi, Veleučilište u Karlovcu, Karlovac 2009; str.36

[2] Šehanović J. i dr.: Informatika za ekonomiste, Sveučilište u Rijeci, Pula 2002., str. 50

2.2. Elementi informacijskog sustava

Da bi uspješno obavljao spomenute funkcije i ostvario navedene ciljeve, informacijski sustav posjeduje određenu strukturu, koja najopćenitije gledano, predstavlja sintezu pet neophodnih elemenata, a to su:[3]

- HARDWARE – materijalna osnovica koju čine informacijske tehnologije (računalo, radne stanice, modemi,fizičke linije za komunikaciju, satelit,...);
- SOFTWARE – nematerijalni elementi u obliku programskih rješenja, rutina, metoda na kojima se temelji primjena hardwarea;
- LIFEWARE – ljudi koji rade s informacijskim tehnologijama bilo kao profesionalni informatičari ili krajnji korisnici;
- ORGWARE – organizacijski postupci, metode i načini povezivanja prethodne tri komponente u skladnu, funkcionalnu cjelinu;
- NETWARE – koncepcija i realizacija komunikacijskog povezivanja, fizičkog i informacijskog, svih elemenata sustava u skladnu cjelinu. Garancija uspješnosti informacijskog sustava je povezivanje navedenih elemenata u kvalitativno podjednaku razinu te njihovo međusobno usklađivanje, a to znači da sam hardware ne rješava probleme već mu u tome pomažu programska rješenja (software). Ali niti to nije dovoljno samo za sebe jer bez dobre organizacije tehnologija je nemoćna. A dobru organizaciju čine educirani, osposobljeni, motivirani zaposlenici koji znaju koristiti i efikasno primijeniti informacijske tehnologije.

2.3. Odnos organizacijskog sustava i njegovog informacijskog podsustava

Informacijske tehnologije svojim eksplozivnim razvojem utječu na brz razvoj informacijskih sustava. Nasuprot njih organizacijski sustav se relativno sporo mijenja i sporo prilagođava na promjene, a ukoliko se tim promjenama svjesno i sistematično ne upravlja dokazano je da se organizacijski sustav neće prilagoditi i tada moderne informacijske tehnologije i rješenja, nov informacijski sustav ostaje strano tijelo unutar poslovnog sustava koje ne povećava njegovu dobit već stvara dodatne troškove. Početak svakog promišljanja o izgradnji novog ili poboljšavanju postojećeg informacijskog sustava je dobro razumijevanje suštine

[3] Luić Lj.: Informacijski sustavi, Veleučilište u Karlovcu, Karlovac 2009; str.37

informacijskog sustava i njegovog odnosa spram objektnog sustava (poduzeća, ustanove) za koji se on gradi. Svaki objektni sustav (OS), koji već postoji, ima svoj informacijski sustav (IS), jer inače ne bi mogao postojati i djelovati. Drugi je problem da li tehnološka razina postojećeg informacijskog sustava predstavlja kritični faktor veće uspješnosti poslovnog sustava. Svaki informacijski sustav (IS) mora biti model poslovne tehnologije (MP) objektnog sustava u kojem radi. Nepodudarnost poslovne tehnologije i informacijskog sustava koji nije strateški ispravno postavljen najveći je razlog neuspješnosti primjene informacijskih tehnologija. [4]

[4] Ibidem; str.38

3. INFORMACIJSKA TEHNOLOGIJA U POSLOVANJU

Informacijska sigurnost u prvom redu asocira na primjenu u IT sektoru, no radi se o puno širem pojmu od toga. U ovom poglavlju objasniti će se uloga informacijske tehnologije u poslovanju. Informacijska tehnologija (IT) mijenja način života i rada ljudi, a također i ustroj te način poslovanja svih gospodarskih subjekata. Neprilagodljivi tim promjenama koje IT donosi, bilo da se radi o poslovnim organizacijama, državnoj upravi ili pojednicima, dovest će u pitanje svoju egzistenciju te uspješno funkcioniranje u novonastalom poslovnom i tehnološkom okruženju.

Prema autoru., tehnološki i poslovno orijentirani ljudi često imaju potpuno različite vizije o tome što predstavlja IT za tvrtku i kako u punoj mjeri iskoristiti njezin potencijal. Na jednoj strani nalazi se poslovodni menadžment koji često ne poznaje dovoljno suvremene informacijske tehnologije, njihove mogućnosti i ograničenja, pa zbog toga ne može izaći iz ustaljenih obrazaca poslovanja, koji se mijenjaju pod utjecajem novih tehnoloških trendova. Na drugoj strani su ljudi orijentirani isključivo na tehnologiju, koji često nemaju dovoljno sluha za poslovne potrebe, sa kupcima i korisnicima orijentiranim na poslovne procese. Zbog toga javlja se nesklad upravljanja s IT-om. IT često zna biti organizirana unutar tvrtki na neadekvatan način, a to izaziva nezadovoljstvo i neispunjenjem očekivanja od rezultata primjene IT.[5]

Ovdje se ne može ni zanemariti informacijska sigurnost, jer isto postoje ljudi unutar organizacije koji nemaju dovoljno sluha za informacijsku sigurnost.

3.1. Menadžment i ulaganje u informacijsku tehnologiju

Ulaganje u informacijsku tehnologiju predstavlja sve veći dio investicija tvrtki. U razvijenim zemljama iznos ulaganja u IT je značajan, pogotovo kada su u pitanju uslužne tvrtke, jer priroda njihovih proizvoda ili učinaka su usluge i informacije. IT kapitalna ulaganja su se od 1980. godine gotovo udvostručila te se očekuje i njihov daljnji rast.

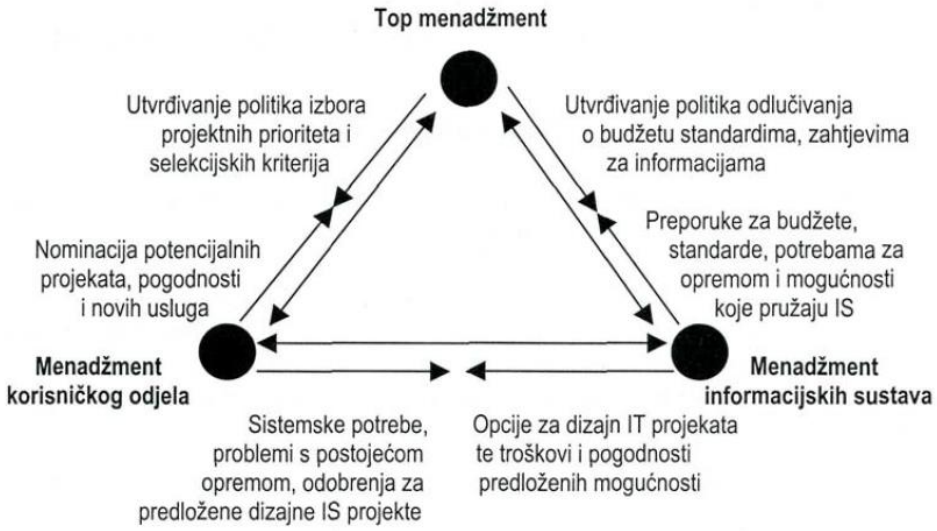
U takvom ozračju ubrzanog rasta važnosti IT, logično je da ona predstavlja temu koja je izuzetno prisutna u suvremenom poslovanju i pridavanje sve veće važnosti načinu ulaganja u informacijsku tehnologiju u tvrtkama i upravljanju njome. Ulaganja u IT uzimaju sve veći

[5] Mueller J., „Upravljanje informacijskom tehnologijom u suvremenim tvrtkama te hrvatska poslovna praksa korištenja informacijskih tehnologija“, Ekonomski pregled, Vol. 52, No. 05-06, 2001, str. 587-612

postotak u ukupnim ulaganjima tvrtki i svi se zapravo pitaju koliko su ona opravdana, a sa druge pak strane, upotrebom suvremene IT tvrtke mogu steći određene konkurentne prednosti kojima mogu potpuno potisnuti i marginalizirati konkurenciju na tržištu.[6]

Zbog toga se nameće potreba kvalitetnog upravljanja informacijskom tehnologijom u suvremenim tvrtkama i njegove organizacije na način da iznosi najveću moguću vrijednost za poslovanje. Tako slika 1. prikazuje na koji bi način u tvrtci morao funkcionirati model upravljanja informacijskom tehnologijom (IT) i informacijskim sustavima (IS).

Slika 1. Kontekst funkcioniranja odjela informatike i model upravljanja IS-om tvrtke



Izvor:Mueller J., „Upravljanje informacijskom tehnologijom u suvremenim tvrtkama te hrvatska poslovna praksa korištenja informacijskih tehnologija“, Ekonomski pregled, Vol. 52, No. 05-06, 2001, str. 587-612

Stalna komunikacija između top menadžmenta i menadžmenta koji koristi IT - menadžment informacijskih sustava, potrebna je kako bi se u tvrtci upravljalo informacijskom tehnologijom na zadovoljavajući način. U cjelokupan proces moraju biti uključeni i sami korisnici sustava koji kroz komunikaciju pomoću IT tehnologije povećavaju performance svojih radnih procesa. Funkciju upravljanja informacijskim sustavima veoma je teško izdvojiti u posebnu jedinicu pri evaluaciji njezinih učinaka i utjecaja na cjelokupno poslovanje.

Informacijska tehnologija predstavlja potpornu djelatnost svim poslovnim funkcijama i poslovnim procesima te predstavlja mogućnost unapređenja njihova funkcioniranja.

[6] Mueller J., „Upravljanje informacijskom tehnologijom u suvremenim tvrtkama te hrvatska poslovna praksa korištenja informacijskih tehnologija“, Ekonomski pregled, Vol. 52, No. 05-06, 2001, str. 587-612

3.2. Odnos između informacijske tehnologije i poslovnih potreba

Odnos između informacijske tehnologije i poslovnih potreba, tj. kvalitetno usklađivanje i ravnoteža između mogućnosti koje pruža IT, s jedne strane, i unapređenja poslovanja, poslovnih funkcija i procesa, sa druge strane, veoma je bitan element uspjeha u suvremenim tvrtkama. Pritom je imperativ pobrinuti se i osigurati da informatički odjel i menadžer informatike (eng. *CIO - Chief Information Officer)* dodaju vrijednost poslovanju. Tako možemo nabrojati kojih bi se sedam načela morao držati CIO, da bi maksimirao dodanu vrijednost informacijske tehnologije u poslovanju:[7]

1. Stalan i neprekidni fokus na poslovne imperative pri razmatranju ulaganja u IT.
2. Interpretacija i benchmark uspješnih praksi implementacija IT s velikim doprinosima poslovnim rezultatima.
3. Ustanovljivanje i održavanje odnosa s CEO (*eng. Chief Executive Officer*) i ostalim top menadžerima.
4. Ustanovljivanje i komuniciranje uspješnih praksi i povijesti funkcioniranja odjela informatike.
5. Koncentracija truda IS odjela na nekoliko glavnih projekata - pravaca.
6. Postizanje zajedničke i izazovne vizije o ulozi IT u budućem poslovanju.
7. Ostvariti kroz IS funkciju značajni poslovni doprinos.

Ova načela odnose se i na CISO- menadžera informacijske sigurnosti (*eng. Chief Information Security Officer*), jer je informacijska sigurnost usko vezana za informacijsku tehnologiju u poslovanju.

O percepciji informacijske tehnologije i njezinih mogućnosti, od glavnih menadžera (CEO) uvelike ovisi koji će tretman dobiti IT u kompaniji. Tako CEO može informacijsku tehnologiju vidjeti kao strateški resurs i sredstvo ostvarenja konkurentske prednosti ili kao običan trošak koji je stoga potrebno svesti na minimalnu moguću mjeru. IS odjel tvrtke mora gledati poslovne jedinice kao kupce svojih usluga tj. informacijske tehnologije i identificirati mogućnosti unapređenja njihovog funkcioniranja. Stoga je bitna funkcija pri upravljanju informacijskim sustavima danas znati prodati ideju biznis menadžmentu i opravdati novac koji je potreban za

[7] Mueller J., „Upravljanje informacijskom tehnologijom u suvremenim tvrtkama te hrvatska poslovna praksa korištenja informacijskih tehnologija“, Ekonomski pregled, Vol. 52, No. 05-06, 2001, str. 587-612

isporuku tehnologije i informacija kompaniji. Potreba za takvim pristupom dolazi iz rezoniranja, prema kojem se smatra da IS odjel nema svoj novac, već koristi novac drugih, pa stoga mora imati kupce u obliku poslovnih odjela koji očekuju određenu vrijednost, tj. povrat na novac koji su uložili. To daje IS funkciji proaktivnu i poduzetničku ulogu unutar kompanije u sklopu koje je ona u stalnoj potrazi za novim kupcima i mogućim projektima koji obećavaju zadovoljavajući povrat uloženih sredstava. Dakle, generalno se može reći da tehnologija i informacijski sustavi sami po sebi nemaju nikakve vrijednosti bez primjene na poslovanje i kreiranja opipljivih pogodnosti i povrata na investicije (novi prihodi, povećani profiti ili nove prilike). Zato je kooperacija između ljudi koji se bave informacijskom tehnologijom i onih koji su orijentirani na poslovanje potrebna da bi IS funkcija dodavala i kreirala adekvatnu vrijednost i pomoć u poslovanju.[8]

3.3. Informacijske tehnologije i strateško planiranje

Prema Muelleru J., planiranje informacijskih sustava tvrtke svakako bi moralo biti sastavnim dijelom poslovnog plana tvrtke. Prije 10-ak godina, samo 36% top menadžera (CEO) tvrtki smatralo da razvitak informacijskih sustava valja podržavati i da on mora biti inkorporiran u poslovni plan cjelokupne tvrtke. Zbog povećanog značaja informacijskih tehnologija i Interneta te sve većeg broja mogućnosti koje oni donose za doprinos i poboljšanje poslovanja, u današnjim uvjetima poslovanja suvremene svjetske tvrtke sebi to sigurno više ne mogu dopustiti, jer IS odjeli postaju generatori promjena i inovacija pa su uključeni u sve bitnije strateške inicijative da bi iznijeli mogućnosti koje pruža IT, a koje iz osnova mogu promijeniti perspektive i poglede na moguće strateške pravce i rješavanja poslovnih problema. Strateško je planiranje IS, dakle, integralni dio sveukupnog strateškog planiranja u tvrtci. Tako se na slici 2., npr., može vidjeti proces koji ilustrira jedan od načina integracije IT u proces poslovnog planiranja.

Pri planiranju i ulaganju u informacijske sustave (IS) uzima se u obzir šest tipova strateških problema[9]:(1) usklađivanje IS s poslovnim prioritetima, (2) arhitekturu IS, (3) infrastrukturu

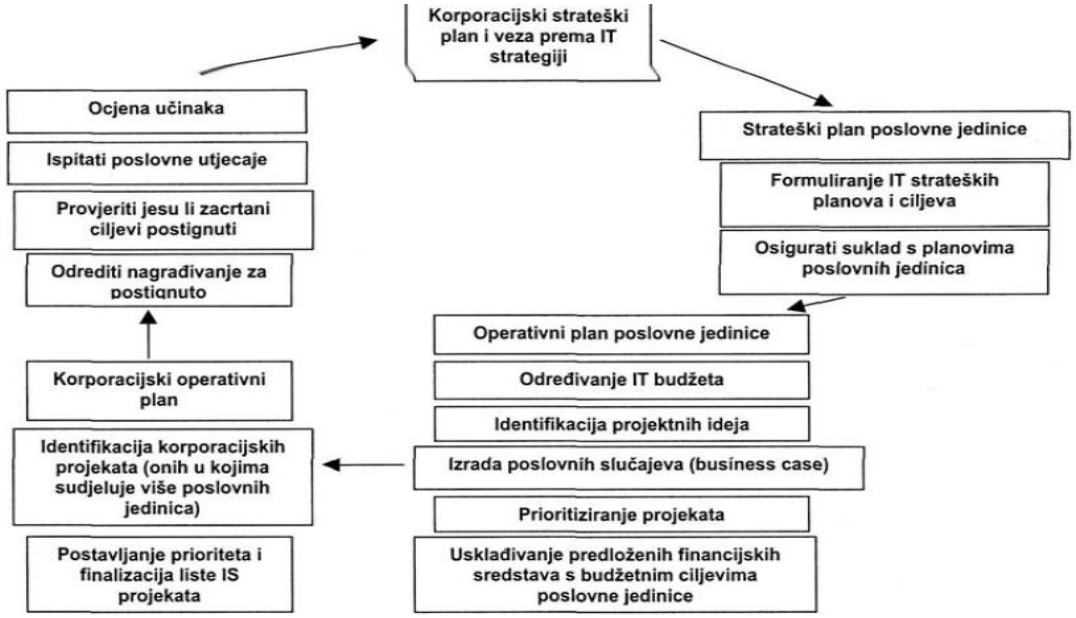
[8] Mueller J., „Upravljanje informacijskom tehnologijom u suvremenim tvrtkama te hrvatska poslovna praksa korištenja informacijskih tehnologija“, Ekonomski pregled, Vol. 52, No. 05-06, 2001, str. 587-612

[9] Ibidem;.

IS, (4) centralizaciju nasuprot decentralizacija, (5) outsourcing (analiza hoće li se i što eksternalizirati), (6) internacionalna pitanja (kompatibilnost, lokalizacija - posebno za multinacionalne tvrtke).

Slika 2.

Integracija IT u proces poslovnog planiranja



Izvor: Mueller J., „Upravljanje informacijskom tehnologijom u suvremenim tvrtkama te hrvatska poslovna praksa korištenja informacijskih tehnologija“, Ekonomski pregled, Vol. 52, No. 05-06, 2001, str. 587-612

Bez integracije IT u proces strateškog planiranja i bez uzimanja u obzir strateških smjernica i ciljeva kompanije pri planiranju njezinih IS, izvjesno je da bi učinak IT na poslovanje tvrtke bio potpuno promašen i neusklađen s poslovnim potrebama. Zato strateško promišljanje orijentirano na poslovne potrebe mora karakterizirati sve važnije odluke o ulaganju i upravljanju informacijskom tehnologijomu suvremenim tvrtkama. Također, sve važnije mjesto pri ulaganju i upravljanju informacijskom tehnologijom zauzima i informacijska sigurnost.

3.4. Preporuke pri ulaganju u informacijsku tehnologiju

Rijetko koji top menadžer zna i razumije zašto ulaganja u IT nisu ispunila očekivanja i kako u budućnosti poboljšati IT. Teško je izračunati cjelokupnu vrijednost IT-a za tvrtku, jer je IT jednostavno previše integrirana u poslovanje da bi se izolirala kao posebna varijabla. Razlika između uspješnih i neuspješnih tvrtki je u percepciji IT u organizaciji. U budućnosti će se vjerojatno jaz između uspješnih i neuspješnih tvrtki još više povećavati. Loše IT tvrtke mogu postati bolje, ali moraju promijeniti svoju percepciju IT-a. Umjesto da informacijsku tehnologiju smatraju ograničenim zadatkom specijalista, IT mora postati predmetom zanimanja top menadžmenta u organizaciji. Od sredstva za reduciranje troškova automatizacijom, IT mora postati oruđe za optimizaciju poslovnih procesa.

Postoje i druge definicije osnovnih faktora uspjeha pri upravljanju informacijskom tehnologijom u tvrtkama, također zasnovanih na istraživanju i iskustvima njihovih autora. Promotrimo jednu koja iznosi zajedničke principe koje dijele tvrtke s visoko učinkovitom upotrebom IT-a (IT-smart organizacije)[10]:

- Učiniti IT poslovno vođenu linijsku aktivnost (uključenost korisnika) umjesto tehnološki vođene odjelske funkcije,
- IT je područje interesa top menadžmenta. (U prosjeku, top menadžment u uspješnim tvrtkama troši mjesečno 45 sati na probleme vezane uz IT, a menadžment manje uspješnih tvrtki troši oko 20 sati. Uspješne tvrtke uz to integriraju svoje IT planove u poslovne planove i procese).
- Učiniti IT odluke vezane uz novčana sredstva poput drugih poslovnih odluka - na osnovi proizvedene vrijednosti.
- Uvoditi jednostavnost i fleksibilnost u tehnološkom okruženju.
- Zahtijevati kratkoročne rezultate od razvojnih projekata i aktivnosti.
- Uvoditi stalna godišnja poboljšanja operacijske djelotvornosti i proizvodnosti,
- Izgraditi "poslovno pametne" IT organizacijske odjele i "IT pametne" poslovne organizacije.

Ono što je zajedničko svim faktorima koji utječu na kvalitetno upravljanje IT funkcijom uz primjenu mjera informacijske sigurnosti u suvremenim organizacijama jest stalno fokusiranje na poslovne potrebe i na mogućnosti koje IT pruža u rješavanju poslovnih problema. Razvitak Interneta i elektroničkog poslovanja dodaje još više kompleksnosti u upravljanju IT funkcijom

[10] Mueller J., „Upravljanje informacijskom tehnologijom u suvremenim tvrtkama te hrvatska poslovna praksa korištenja informacijskih tehnologija", Ekonomski pregled, Vol. 52, No. 05-06, 2001, str. 587-612

u tvrtkama, ali ne mijenja tu jednostavnu činjenicu koja postaje sve bitnija za uspješno poslovanje suvremenih kompanija.

3.5. Eksternalizacija (*outsourcing*) informacijske tehnologije

Zbog kompleksnosti i tehničke ekspertize koje zahtijeva, mnoge se tvrtke danas odlučuju na *outsourcing* odnosno eksternalizaciju jednog dijela ili čak cjelokupnog upravljanja informacijskom tehnologijom.

Outsourcing IS funkcije tako se može definirati kao odluka da se preda upravljanje dijelom IS funkcije (ili čak cjelokupnom IS funkcijom) vanjskom pružatelju usluge, a sve to sa svrhom uspješnijeg upravljanja tim aktivnostima i funkcijama. Tako je primjerice, tržište IS outsourcinga u SAD raslo u razdoblju 1988.- 1994. od 22,8 mlrd.USD na iznos od 49,5 mlrd. USD. Pritom se ovdje misli na outsourcing u užem smislu koji sadrži vanjske usluge razvitka i održavanja aplikacija, sistemske operacije, menadžment mrežama/telekomunikacijama, podršku krajnjim korisnicima računala, sistemskog planiranja i menadžment i kupovinu aplikacijskog softvera, ali isključuje usluge poput poslovnog konzaltinga, poslije-prodajne usluge prodavača i iznajmljivanja telefonskih linija[11].

Rastom kompleksnosti i mogućnosti informacijskih sustava i pojavljivanjem kompleksnih rješenja, poput sustava za planiranje resursa tvrtki (*ERP – Enterprise resource planing systems*), dio vezan uz poslovni konzalting i potporu i nadogradnju sustava nakon njegove kupovine i instalacije, predstavljaju sve značajniji dio ulaganja suvremenih tvrtki u outsourcing IT. Razvitak vlastitih softverskih rješenja za rješavanje većih i značajnijih problema nije se pokazao kao najsretnije rješenje, pa tako teško da će neka moderna tvrtka ući u izgradnju vlastitog ERP ili neke druge velike aplikacije prvenstveno zbog prevelikih ulaganja u vlastite djelatnike. Primjer toga je sam Microsoft koji je svoj vlastiti ERP saustav kupio od SAP-a (vodeće tvrtke za razvoj ERP saustav u svijetu).

Prema Muelleru J. mogući razlozi za outsourcing IT su:[12] reduciranje troškova i injekcija gotovine prodajom imovine ili transfer IS osoblja vanjskom davatelju usluga; brži razvitak IT aplikacija; poboljšanje kvalitete usluga i proizvodnosti; pristup vodećim i novim tehnološkim rješenjima i kompetencijama; reduciranje tehnološkog rizika i povećanje fleksibilnosti

[11] Mueller J., „Upravljanje informacijskom tehnologijom u suvremenim tvrtkama te hrvatska poslovna praksa korištenja informacijskih tehnologija“, Ekonomski pregled, Vol. 52, No. 05-06, 2001, str. 587-612

[12] Ibidem;

upravljanja IT resursima; brža implementacija promjena; provjera i preispitivanje trenutnih praksi i problematičnih slučajeva upravljanja s tehnologijom i informacijama iz neovisnog izvora (pružaoca usluge); olakšanje upravljanja IS funkcijom senior menadžmentu.

Isti autor navodi i moguće razloge i rizike koji su usmjereni protiv outsourcinga IT-a, a to su: mogući povećani troškovi u dužem roku; povećani rizik pri upravljanju IS funkcijom; gubitak internog IT znanja i kritičnih vještina; mogući gubitak fleksibilnosti u dugom roku zbog velike ovisnosti o pružatelju IS *outsourcing* usluga (preveliki troškovi promjene dobavljača usluge); povećanje kompleksnosti upravljanja i koordinacijom IS funkcija i usluga i gubitak kontrole nad IT odlukama, podacima i sigurnosnim pitanjima; kršenje ugovora ili nemogućnost isporuke dogovorenoga pružaoca usluga; gubitak kontrole nad pružaocem usluga i nekontrolirani rast ugovora i postojanje "sakrivenih troškova" koje tvrtka ne uviđa; nedostatak povjerenja između tvrtke pružaoca i primaoca IT outsourcing usluga.

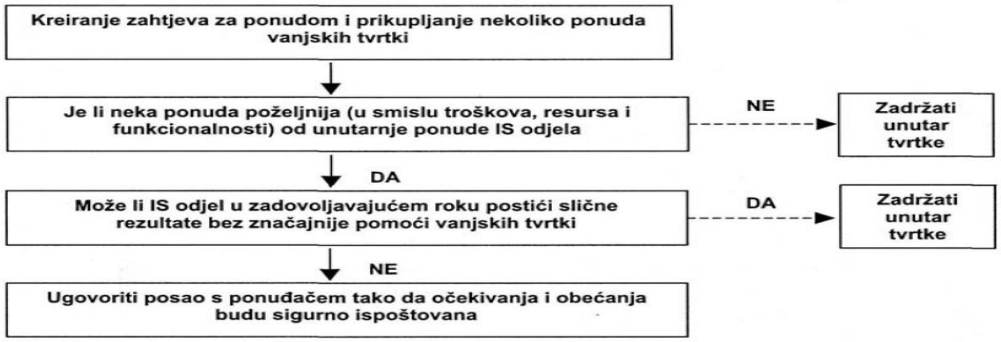
Rezultati istraživanja o korištenju IT *outsourcinga* u američkim tvrtkama koje je provedeno godine 1995. u SAD : proizvođačke su tvrtke eksternalizirale svoju IS funkciju u nešto većem postotku od tvrtki iz uslužnih djelatnosti; voditelji informatičkih službi igraju veoma značajnu ulogu pri odluci hoće li ući u IS outsourcing; tvrtke s manjim IS budžetima manje ulaze u IS outsourcing, vjerojatno zbog činjenice da su potrebna veća sredstva da bi outsourcing bio isplativ; tvrtke s decentraliziranijom IS funkcijom više podležu outsourcingu IS; značajan postotak tvrtki - 77% je izjavilo da provode outsourcing jedne ili više IS funkcija, a globalni outsourcing (pružatelj usluge - tvrtka izvan SAD) postoji kod 17% ispitanika.[13]

Proces odluke da li eksternalizirati IS usluge ili ne, prikazan je na slici 3.

[13] Ibidem;

Slika 3.

Proces odlučivanja hoćemo li ekaternalizirati IS uslugu ili projekt



Izvor: Mueller J., „Upravljanje informacijskom tehnologijom u suvremenim tvrtkama te hrvatska poslovna praksa korištenja informacijskih tehnologija“, Ekonomski pregled, Vol. 52, No. 05-06, 2001, str. 587-612

Tako se na kraju može iznijeti i ovo: preporuku suvremenih tvrtki pri razmatranju i mogućoj realizaciji *IT outsourcinga*:[14]

1. Razumjeti unutarnje snage i slabost informacijskih sustava i IS odjela tvrtke.
2. Postati što je moguće više upoznat s IT industrijom, s njezinim trendovima i posebno sa tvrtkama pružateljima *IS outsourcing* usluga.
3. Postepeno razviti poslovni odnos s jednim ili više dobavljača IS usluga.
4. Jasno razumjeti poslovne ciljeve koji moraju biti postignuti *IS outsourcingou*.
5. Prepoznati da su promjene neminovne i konstantno im se prilagođivati u odnosu s pružaocima IS usluga.

U seriji normi ISO 27000, detaljno je objašnjeno na što sve treba obratiti pažnju i koje radnje su potrebne prilikom eksternalizacije bilo koje funkcije u organizaciji, odnosno kako nastupiti prema *outsourcing* tvrtci.

[14] Mueller J., „Upravljanje informacijskom tehnologijom u suvremenim tvrtkama te hrvatska poslovna praksa korištenja informacijskih tehnologija“, Ekonomski pregled, Vol. 52, No. 05-06, 2001, str. 587-612

3.6. Isplativost ulaganja u informacijsku tehnologiju

Ulaganje u IT i informacijsku sigurnost te isplativost tih ulaganja intenzivan su predmet razmatranju posljednjih dvadesetak godina. Tako Mueller J. navodi da jedan od najvećih kritičara ulaganja u IT i osobna računala, Paul Strassmann koji u svojoj knjizi "Protraćeno računalo" *(Squandered Computer*) izražava svoje sumnje o povezanosti iznosa ulaganja u IT i o profitabilnosti poslovanja. Kao primjer za argumentaciju dotične tvrdnje, Paul Strassmann navodi rezultate istraživanja koja pokazuju odnos između ulaganja u IT i prihoda po dionicama i odnos između ulaganja u IT i profitabilnosti poslovanja u proizvodnim poduzećima i u bankarskoj industriji. Isti rezultati istraživanja nisu pokazali izravnu korelaciju između spomenutih kategorija. Na osnovi toga zaključuje da razliku ne čine računala, nego ljudi koji s njima rade. Rezultat je više nego logičan, a i sam autor navodi da nije bilo ni logično očekivati korelaciju između istraživanih veličina jer je informacijska tehnologija samo katalizator. Ono što proizvodi poslovne rezultate jesu dobro obrazovani, organizirani i motivirani ljudi koji znaju na koji način iskoristiti nove pogodnosti što ih pružaju informacijska tehnologija i ulaganja u nju.[15]

[15] Ibidem;

4. INFORMACIJSKA SIGURNOST

Sigurnost informacijskih sustava bitna je tema kojoj organizacije diljem svijeta pridaju mnogo pažnje za što postoji i dobar razlog. Sigurnosne prijetnje dolaze iz više izvora poput računalnog kriminala, špijunaže, sabotaža i prirodnih nepogoda. Šteta nanesena od strane računalnog kriminala sve je veća što pokazuju financijski pokazatelji pa je bitno definirati, planirati, projektirati, implementirati, održavati i kontinuirano poboljšavati informacijsku sigurnost.
Područja informacijske sigurnosti za koja se propisuju mjere i standardi informacijske sigurnosti su:[16]
– sigurnosna provjera,
– fizička sigurnost,
– sigurnost podatka,
–sigurnost informacijskog sustava,
– sigurnost poslovne suradnje.

Prema Zakonu o informacijskoj sigurnosti, I. Osnovne odredbe, Članak 2. navodi:[17]
„Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.“
Osim zakona informacijska sigurnost definirana je i ISO 27001 standardom:[18]
Informacijska sigurnost podrazumijeva očuvanje povjerljivosti, integriteta i dostupnosti informacije; uključiti se mogu i druge osobine kao što su vjerodostojnost, odgovornost, neporecivost i pouzdanost. Uz ovaj pojam ISO 27001 definira sljedeće pojmove bitne za ovo područje:[19]

- **sigurnosni događaj** je prepoznatljiv slučaj stanja sustava, usluge ili mreže koji upućuje na moguću povredu politike informacijske sigurnosti ili neuspjeh zaštite ili do tada nepoznate okolnosti koje mogu biti važne za sigurnost;

[16] Zakon o informacijskoj sigurnosti, NN 79/07

[17] Zakon o informacijskoj sigurnosti, NN 79/07

[18] Kostanjevec A. i dr.. Sigurnost informacijskih sustava verzija 01012014, FOI Varaždin 2014. str.2.

[19] Ibidem;

- **sigurnosni incident** naznačen je jednim ili nizom neželjenih ili neočekivanih sigurnosnih događaja koji imaju značajnu vjerojatnost ugrožavanja poslovnih aktivnosti i informacijske sigurnosti;
- **zaštita,** kao nositelja svih informacija potrebnih za nesmetan rad poslovnog sustava. Zaštita podrazumijeva provođenje mjera poradi osiguranja informacijskog sustava.[20]
- **ranjivost.** Budući da je sustav ranjiv, pa tako postoji rizik da informacija bude izložena neovlaštenom pristupu. ISO 27002 ranjivost definira kao:[21] „Ranjivost je slabost imovine ili grupe imovina koju jedna ili više prijetnji mogu iskoristiti.“ Općenito možemo ranjivosti podijeliti na ranjivosti aplikacije i ranjivosti operacijskog sustava.
- **rizik**. ISO 27001 pri opisu upravljanja informacijskom sigurnošću ISMS navodi kako je dio cjelokupnog sustava upravljanjem, temeljen na pristupu sa strane poslovnih rizika, kako bi uspostavio, implementirao, nadzirao, provjeravao, održavao i unapređivao informacijsku sigurnost. (*NAPOMENA: Sustav upravljanja uključuje organizacijsku strukturu, politike, planiranje aktivnosti, odgovornosti, vježbe, procedure, procese i resurse*.) Rizik je u literaturi definiran kao funkcija razine prijetnje, ranjivosti i vrijednosti informacijske imovine. izik se jasnije može opisati kao vjerojatnost prijetnje da iskoristi neku ranjivost imovine te time ugrozi imovinu. S obzirom na navedene definicije rizik je moguće prikazati matematičkom formulom:

  RIZIK = PRIJETNJA * RANJIVOST * VRIJEDNOST IMOVINE

  Prikazanom formulom ne izračunava se rizik već formula služi za shvaćanje međuovisnosti prijetnje, ranjivosti i vrijednosti imovine na razinu rizika. Postoji li visoka razina prijetnje i visoka razina ranjivosti, razina rizika je visoka. Kada je razina prijetnji visoka, ali poduzeće nije toliko ranjivo jer ima implementiranu prikladnu zaštitu tada će razina rizika biti srednja. Poduzeće također može posjedovati imovinu male vrijednosti. Ako u tom slučaju dođe do sigurnosnog incidenta poduzeće neće pretrpjeti velike gubitke, pa rizik nije visok.

  U normi ISO 27001 su definirani još neki bitni pojmovi vezani uz ovo područje:[22]

  Integritet - Osobina očuvanja autentičnosti i cjelovitosti imovine

  Rezidualni rizik - Preostali rizik nakon obrade rizika

  Prihvaćanje rizika -Odluka da se rizik prihvati

  Analiza rizika - Sustavna uporaba informacija za određivanje izvora i procjenu rizika

[20] Boban M, Perišić M., , Zbornik radova Veleučilišta u Šibeniku, No.1-2/2015, srpanj 2015, str. 115-148

[21] Kostanjevec A. i dr.. Sigurnost informacijskih sustava verzija 01012014, FOI Varaždin 2014. str.2

[22] Ibidem,

Procjena rizika - cjelokupan proces analize rizika i njegovog vrednovanja

Vrednovanje rizika - Proces usporedbe procijenjenog rizika s danim kriterijima, kako bi se ustanovio značaj rizika.

Upravljanje rizikom - Usklađene aktivnosti za usmjeravanje i kontrolu organizacije u smislu rizika.(*NAPOMENA: Izraz "kontrola" korišten je kao sinonim za mjera.)*

Obrada rizika - Proces odabira i primjene mjera za promjenu rizika.

- **prijetnja** (*engl. Threat*) je potencijal za povredu sigurnosti, koji postoji ako postoje okolnosti, mogućnost, akcija ili događaj koji može ugroziti sigurnost i prouzrokovati štetu.
- **napad** (*engl. Attack*) je definiran kao napad na sigurnost sustava koji proizlazi iz inteligentne prijetnje; to jest inteligentni čin koji predstavlja namjerni pokušaj (pogotovo u smislu metode ili tehnike) da se izbjegne sigurnosne servise i prekrši sigurnosna politika sustava.
- **sigurnosni napad** je akcija koja kompromitira sigurnost informacija posjedovanih od strane organizacije.
- **sigurnosni servis** povećava sigurnost sustava za obradu podataka i prijenos informacija u organizaciji. Namjena servisa je suprotstavljanje sigurnosnim napadima. Servis koristi jedan ili više sigurnosnih mehanizama kako bi osigurao pružanje usluge.
- **vektor napada** je put ili sredstvo kojim napad može biti ili je napravljen na kritičnom djelu infrastrukture. Drugim riječima vektori napada omogućuju hakerima da iskoriste ranjivosti sustava, uključujući i ljudske pogreške.
- **sigurnosni mehanizam** je mehanizam dizajniran za otkrivanje, sprečavanje i oporavak od sigurnosnih napada.

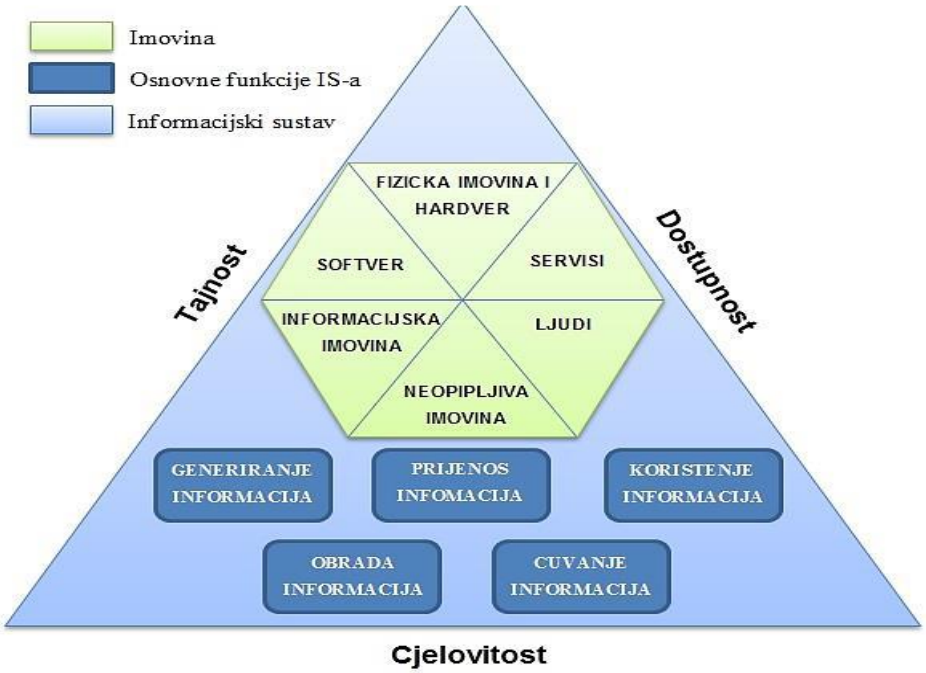
4.1. CIA teorem

Kako bi se informacijski sustav mogao zaštiti potrebno je znati što je bitno zaštititi. Uz funkcije informacijskog sustava potrebno je osigurati samu informaciju i to njene tri značajke:[23]

- Tajnost (*engl. Confidentiality)*
- Cjelovitost (*engl. Integrity)*
- Dostupnost (*engl. Availability*)

Informacijski sustav pomoću svoje imovine mora osigurati sve ili barem neke radne funkcije, ali obavezno konzistentnost sve tri značajke svih informacija u njemu.

Slika 4.Odnos informacijskog sustava i značajki informacija



Izvor: Kostanjevec A., et al.: Sigurnost informacijskih sustava verzija 01012014, FOI Varaždin, Varaždin, 2014. str.1.

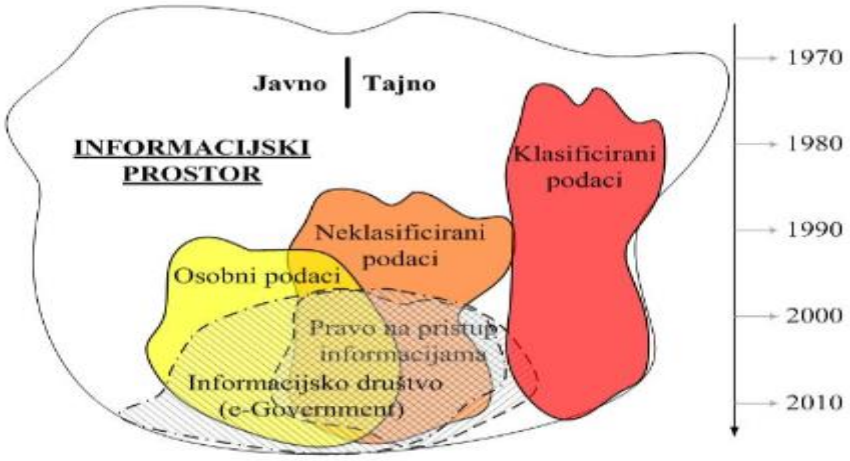
Iz navedenog prikaza proizlazi da se informacijski sustav može prikazati kao skup: IS={CIA, Imovina, Funkcije}. Dakle, informacijski sustav se sastoji od imovine (fizička imovina, softver itd.), ljudi te funkcija IS-a (prijenos informacija, korištenje informacija, čuvanje informacija itd). U IS-u potrebno je očuvati cjelovitost, tajnost i dostupnost.

[23] Ibidem. str. 1.

4.2. Informacijski prostor

Informacijski prostor predstavlja virtualnu globalnu okolinu međusobno povezanih javnih i privatnih informacijski sustava u kojoj nastaju i prenose se različite vrste podataka, ali i specifični podaci koji su dominantni s obzirom na propise i zahtjeve informacijske sigurnosti. Slijedom toga potrebno je primijeniti mjere i standarde informacijske sigurnosti propisane za zaštitu povjerljivosti, dostupnosti i cjelovitosti podataka te dostupnosti i cjelovitosti informacijskih sustava u kojima se ti podaci obrađuju, pohranjuju ili prenose. Suvremeni informacijski prostor stvara se tijekom posljednjih nekoliko desetljeća. U tom razdoblju čitav niz različitih trendova utjecao je na formiranje suvremene paradigme informacijskog društva i pripadajućeg informacijskog prostora. Analizom razdoblja od posljednjih nekoliko desetljeća mogu se utvrditi neke karakteristične faze kroz koje je oblikovanje javnog informacijskog prostora prolazilo, kao što je prikazano na Slici 5.[24]

Slika 5: Stvaranje suvremenog informacijskog prostora



Izvor:Klaić A., Perešin A.:Zbornik radova; Dani kriznog upravljanja 2011. 678-708. str. Veleučilište Velika Gorica 2011

[24] Klaić A., Perešin A.: Zbornik radova; Dani kriznog upravljanja 2011. 678-708 str. Veleučilište Velika Gorica 2011.

Podjela informacijskog prostora

U razdoblju do sedamdesetih godina prošlog stoljeća, kako je prikazano na Slici 5., informacijski prostor karakterizirala je izražena segmantacija informacijskog prostora u okviru pojedinih država, kao i oštra granica između javnog i tajnog informacijskog prostora. Ova oštra granica u to je vrijeme bila dodatno naglašena diskrecijskom mogučnošću odlučivanja državnih tijela o granicama između javnog i tajnog dijela informacijskog prostora. Tajni prostor pripadao je u potpunosti državnom sektoru u užem smislu, odnosno najvećim dijelom sigurnosno – obavještajnom, policijskom i vojnom dijelu tog sektora, a pravila klasificiranja podataka bila su gotovo potpuno zatvorena za širu javnost. Nužnost vojne, ali i obavještajno- sigurnosne suradnje između različitih država, sve više je profilirala postupke klasificiranja podataka te se ne prijelazu sedamdesetih u osamdesete godine prošlog stoljeća sve jasnije utvrđuju koncepti, danas široko prihvaćene četvero-stupanjske klasifikacije tajnosti podataka, temeljene na stupnju štete od neovlaštenog otkrivanja klasificiranog podatka. Bitna komponenta ovog koncepta bila je jasna veza između stupnja tajnosti određenog klasificiranog podatka i skupa mjera i standarda informacijske sigurnosti kojima treba zaštititi podatak određenog stupnja tajnosti. Sve jasniji zahtjevi sigurnosne politike u šezdesetim i sedamdesetim godinama prošlog stoljeća potiču stvaranje sigurnosnih modela za provedbu ciljeva sigurnosne politike, u prvom redu na informacijskim sustavima. Tako su nastali rešetkasti model *(Lattice Model) i Bell-La Padula model,* formalni sigurnosni modeli koji se bave kontrolom pristupa podacima na informacijskom sustavu, odnosno sigurnosnim kriterijem povjerljivosti tih podataka, ili primjerice *Biba model* koji je usmjeren na kriterij cjelovitosti podataka. Sigurnosnim modelima, na formalni, matematički način, arhitektura informacijskog sustava prilagođava se ciljevima sigurnosne politike. S obzirom da je sastavni dio informacijskog sustava u primjeni i njegovo okruženje, koje uz tehnički sustav obuhvaća i podatke na sustavu te korisnike sustava, nužan korak dalje bili su sigurnosni načini rada informacijskih sustava. Tako sigurnosni načini rada informacijskih sustava: namjenski (*eng. dedicated*), na razini sustava (*eng. system high*), razdijeljeni (*eng. compartmented*) i multirazinski (*eng. multilevel*), povezuju stupanj tajnosti klasificiranih podataka na informacijskom sustavu, razinu sigurnosnih certifikata osoba koje pristupaju informacijskom sustavu, nužnost pristupa klasificiranom podatku u okviru djelokruga rada osobe (*eng. need-to-know*), kao i formalno odobrenje za pristup podacima na informacijskom sustavu.[25]

[25] Ibidem;

Vidljivo je da uspostava sustava povjerenja prema osobama čini bitan i nužan element provedbe sigurnosne politike. Tako se, primjerice, u državnoj upravi, osobama koje pristupaju klasificiranim podacima, na temelju sigurnosne provjere izdaje sigurnosno uvjerenje (certifikat) odgovarajućeg stupnja tajnosti, usklađenog sa stupnjem tajnosti klasificiranih podataka kojima trebaju pristupati. Postupak sigurnosne provjere inicira državno tijelo, za svog zaposlenika koji u okviru djelokruga svog radnog mjesta ima potrebu pristupa (engl. *need-to-know*) određenim kategorijama klasificiranih podataka kao što su NATO ili EU klasificirani podaci, ili pojedinim nacionalnim kategorijama klasificiranih podataka, kao što su, primjerice, podaci o klasificiranim ugovorima u okviru nabave (princip razdvajanja nadležnosti). Izdavanjem sigurnosnog certifikata osobi te potpisivanjem izjave osobe o tome da je svjesna svojih prava i obveza u području tajnosti podataka, rukovoditelji pojedinih službi izdaju formalno odobrenje za pristup određenom fondu klasificiranih podataka ili odobravaju pristup na neformalnoj razini, razvođenjem pojedinog klasificiranog podatka osobi koja ima odgovarajući certifikat i poslovno zaduženje. Ovakav koncept provedbe sigurnosne politike razvio se u državnim upravama tijekom sedamdesetih i osamdesetih godina prošlog stoljeća, isprva u najrazvijenijim državama svijeta, a kasnije i u ostalim demokratskim državama. Tako dolazi do stvaranja jasne i transparentne regulative vezane uz principe klasificiranja podataka, čime se tajni dio tadašnjeg informacijskog prostora transformirao u relativno transparentno, jasno ograničeno područje, odnosno u domenu klasificiranih podataka. S obzirom da su načela klasificiranja postala slična u različitim državama i pri tome javno propisana i transparentna, stvoreni su preduvjeti za učinkovitu međunarodnu razmjenu klasificiranih podataka i suradnju različitih država na problematici koja zahtijeva razmjenu klasificiranih podataka, kao što je vojna suradnja, ili borba protiv suvremenih ugroza, kao što je terorizam. [26] Tek iznimno brz razvoj informacijske i komunikacijske tehnologije te brzo širenje interneta tijekom devedesetih godina, ublažava nacionalnu segmentaciju informacijskog prostora, povezujući nacionalne informacijske prostore različitih država u zajednički globalni informacijski prostor. No, isto tako, u takvim okolnostima društvo postaje sve više svjesno potrebe zaštite od ugroza povezanih s rastućom i globalnom informacijskom tehnologijom. Bilo je to vrijeme, napose u Europskoj uniji , kada je započela sustavna regulacija općenitih koncepata privatnosti, kao i specifičnosti zaštite osobnih podataka, što je ubrzo postalo globalna paradigma razvijenog svijeta.[27]

[26] Ibidem;

[27] Ibidem;

Na taj je način domena osobnih podataka postala posebno značajna u informacijskom prostoru jer su korisnici osobnih podataka i državna tijela i druge pravne osobe, a osobni podaci često se razmjenjuju u okviru međunarodne suradnje različitih država, ali i u okviru svakodnevnih poslova, kao što je, primjerice, sigurnost zračnog prometa. Općeniti koncepti privatnosti pravnih osoba, odnosno zaštite intelektualnog vlasništva, tradicionalno korišteni u obliku poslovne tajne, tijekom devedesetih godina jasnije se definiraju i u državnom sektoru. Stvaranjem globalnog informacijskog prostora, uvelike temeljenog na rasprostranjenosti i sveprisutnosti interneta, javlja se potreba za učinkovitijim pristupom cjelokupnom informacijskom prostoru, u odnosu na pristup koji proizlazi iz korištenja i načela pojedinih podatkovnih domena informacijskog prostora, kao što je, primjerice, domena klasificiranih podataka. Pored nezaustavljive integracije nacionalnih informacijskih prostora u globalni informacijski prostor, međunarodne i nacionalne potrebe za komuniciranjem nameću promjenu i prilagodbu sigurnosnih politika i prakse komuniciranja s različitim vrstama podataka, kao što su osobni podaci ili klasificirani podaci. Takve promjene nije moguće postići bez opsežne i koordinirane prilagodbe kompleksne regulative u području tajnosti i privatnosti podataka. Upravo to se posljednjih desetak godina i događa te se, počevši od paradigme elektroničke državne uprave, preko šireg pojma informacijskog društva, prilagođavaju komponente nacionalnog zakonodavstva povezane s konceptima tajnosti i privatnosti. [28]

Takve prilagodbe, zbog iznimnog tehnološkog iskoraka u području elektroničkih komunikacija i informacijske tehnologije te sveprisutnosti interneta, kao i posljedično stvorene nove društvene situacije – globalizacije, sežu u čitav niz zakona kojima se regulira područje rada davatelja elektroničkih komunikacijskih usluga, utvrđuju elektroničke inačice dokumenata i potpisa, postavljaju načela zaštite klasificiranih podataka, osobnih i drugih podataka, propisuju mjere i standardi zaštite podataka, odnosno potiče normizacija, kako u tehnološkom, tako i u sigurnosnom smislu. Prilagodba nacionalnog sustava sigurnosnim zahtjevima NATO-a i EU-a, zahtijeva stvaranje koncepta regulativnog okvira informacijske sigurnosti koji će državnom, javnom i privatnom sektoru propisati, odnosno dati smjernice za zaštitu podataka u informacijskom prostoru.[29]

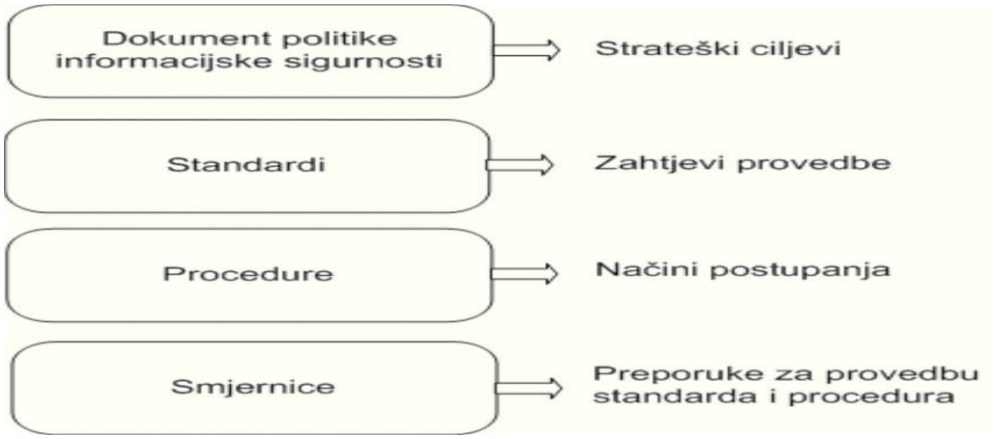
[28] Ibidem;

[29] Ibidem;

4.3. Politika informacijske sigurnosti

Prema Klaić A. i Perešin A. politika informacijske sigurnosti predstavlja dokumente kojima se utvrđuju mjere i standardi informacijske sigurnosti koje je potrebno primijeniti u informacijskom prostoru za zaštitu povjerljivosti, dostupnosti i cjelovitosti podataka te dostupnosti i cjelovitosti informacijskih sustava u kojima se ti podaci obrađuju, pohranjuju ili prenose.[30] Politika informacijske sigurnosti koristi se i kao naziv za izjavu ili očitovanje najodgovornijih osoba (uprava tvrtke, čelnik državnog tijela, ...) o uvjerenjima, ciljevima i razlozima te općenitim načinima kako doći do željenih postignuća u području informacijske sigurnosti, i to u obliku kratkog i konciznog dokumenta na općenitoj razini, bez specifičnosti i detaljnih opisa. Donošenje ovakvih dokumenata sigurnosne politike najčešće proizlazi iz zakonskih obveza, odnosno iz primjene normi kao što je HRN ISO/IEC 27001, a može biti i rezultat vlastite unutarnje inicijative određene institucije. Općenito, politika informacijske sigurnosti predstavlja hijerarhijski strukturiran skup dokumenata koji se, pored opisanog krovnog dokumenta, uobičajeno sastoji i od razine standarda, koji predstavljaju obvezujuće zahtjeve za provedbu sigurnosne politike, razine procedura, koje predstavljaju obvezujuće postupke te od razine smjernica ili naputaka, koje su preporučeni načini realizacije i stvaranja okvira za provedbu standarda i procedura (Slika 6).[31]

Slika 6. Hijerarhijske razine u sklopu dokumenata informacijske sigurnosti



Izvor: Klaić A., Perešin A.:, Zbornik radova; Dani kriznog upravljanja 2011. 678-708. str. Veleučilište Velika Gorica 2011

[30] Ibidem;

[31] Ibidem;

Kompleksnost općeg, krovnog dokumenta politike informacijske sigurnosti pritom ovisi o kompleksnosti organizacije i ciljeva koji se žele postići te su u tom smislu politike informacijske sigurnosti u državnom sektoru često vrlo kompleksne, jer u sebi sadrže i uspostavu mehanizama nužnih za organizaciju i upravljanje informacijskom sigurnošću u iznimno heterogenom okruženju kakvo je državna uprava. Uz sve navedeno, politika informacijske sigurnosti se i funkcionalno raščlanjuje na više slojeva, pa obično razlikujemo opće politike na razini organizacije u cijelosti, funkcionalne politike po određenim područjima (npr. fizička sigurnost), kao i specifične politike te politike prihvatljivog korištenja *(engl. Acceptable Use Policy – AUP)* pojedinih resursa (npr. sustava, aplikacija i sl.) . Bez obzira na razlike u formi dokumenata politike informacijske sigurnosti, pristupu i nazivlju, općenito rečeno, politikom informacijske sigurnosti uvijek se osigurava uvođenje minimalnih sigurnosnih zahtjeva u okviru određene organizacijske cjeline.[32]

4.4. Kibernetska sigurnost

Za pojam *cyber* još ne postoje precizne definicije. Anićev rječnik stranih riječi navodi kako je cyber prvi element u riječima koji označava nešto vezano uz svijet prividne stvarnosti koji nastaje pomoću računala. Prema pojmovniku *National Security Agency (NSA) cyber* je prefiks koji se koristi kako bi se osoba, stvar ili ideja svrstala kao dio računalnog ili informacijskog doba. Za pojam *cyber* još ne postoji ni ustaljen odgovarajući prijevod na hrvatski jezik. Naime, u Republici Hrvatskoj učinjena je terminološka zbrka kada se prevodila konvencija *Convention on Cybercrime*. Hrvatski prijevod konvencije glasi Konvencija o kibernetičkom kriminalu, iako riječ kibernetika (*engl. Cybernetics*) nije istoznačnica riječi *cyber*. Stoga neki autori smatraju kako je pridjev „kibernetički“ pogrešan prijevod, te kako se pojam *cyber* treba odvojiti od pojma kibernetika. Kibernetiku bi najkraće mogli definirati kao "sustavno proučavanje komunikacije i upravljanja u organizacijama svih vrsta". Dakle, kibernetika je znanstvena disciplina, a *cyber* se, kako je navedeno u pojmovniku NSA-e, odnosi na svijet koji nastaje pomoću računala. [33]

[32] Ibidem;

[33] Vuković Hrvoje; *National security and the future*, Vol.13, No.3., str. 12-31, Udruga Sv.Jurja Zagreb, rujan 2012.

Kibernetski prostor

U listopadu 2006. Združeni stožer oružanih snaga SAD-a definirao je kibernetski prostor kao „područje koje karakterizira upotreba elektroničkog i elektromagnetskog dijapazona za pohranjivanje, modificiranje i razmjenjivanje podataka putem mrežnih sustava i povezanih fizičkih infrastruktura“. Korisnici kibernetskog prostora poput domaćinstva, korporacija, sveučilišta, vlada, oružanih snaga itd. kreću se kibernetskim prostorom kako bi izgradili ili dostigli informacijska odredišta koja se dijele, stječu i nadziru putem mrežnih sustava u kojima povezanost čine obične telefonske linije, mikrovalni uređaji, satelitske uzlazne i silazne veze, optička vlakna, kablovi, tranzistori i mikročipovi. Internet je najpoznatiji i najrasprostranjeniji mrežni sustav. U kibernetskom prostoru, informacije su dostupne u realnom vremenu i njihova bitna odrednica postaje temporalnost, ovisnost o vremenu, a ne o prostoru. Za brze promijene u kibernetskom prostoru potrebno je vrlo malo vremena.[34]

Ljudi često misle da su informacijski prostor i kibernetski prostor isto, što nije točno. Informacijski prostor širi je pojam od kibernetskog prostora.

Ugroze u kibernetskom prostoru - podjela

Maliciozne kibernetske aktivnosti dijele se na:[35]

1. kibernetski kriminal,
2. kibernetsku špijunažu,
3. kibernetski terorizam i
4. kibernetsko ratovanje.

Kibernetski napadi javljaju se u dvije forme s obzirom na njihov cilj:[36]

1. napad usmjeren na podatke i
2. napad usmjeren na nadzorne sustave.

Krađa i kvarenje podataka dovodi do sabotiranja usluga i to je čest oblik napada putem Interneta i računala. Napadi koji su usmjereni na kontrolne sustave koriste se sa svrhom manipuliranja fizičkom infrastrukturom (npr. opskrbom električnom energijom, željezničkim prometom ili vodnim zalihama). To se čini na način da se putem Interneta ili drugačije penetrira u sustave.

[34] Ibidem;

[35] Ibidem;

[36] Ibidem;

Tako je, na primjer, u ožujku 2000. bivši zaposlenik preko Interneta neovlašteno ušao u elektronički nadzorni sustav pumpi i otpustio milijun litara otpadnih voda u vodni sustav Maroochy Shire u Queenslandu, u Australiji. Trebalo mu je 45 pokušaja da uspješno penetrira u sustav. Dakle, 44 pokušaja ostala su nezamijećena. Jedanaest godina kasnije pojavile su se prve analize Stuxneta, visoko sofisticiranog oblika malicioznog koda sposobnog djelovati neopaženo protiv industrijskih nadzornih sustava dok uništava zadane ciljeve, te kojem više nije potreban Internet da bi inficirao željeni sustav. Potrebno je istaknuti kako fizički oblici kibernetskog terorizma, kibernetskog ratovanja, kibernetske špijunaže i kibernetskog kriminala često izgledaju isto ili slično. Lech J. Janczewski i Andrew M. Colarik navode primjer kada netko provali u bolničku bazu podataka i prepiše lijek pacijentu koji je alergičan na taj lijek. Kao rezultat, pacijent umire. Ako je namjera napadača bila nauditi pacijentu ili ubiti ga iz nekih osobnih razloga, riječ je o kaznenom djelu ubojstva izvedenom pomoću računalne tehnologije, dakle o kibernetskom kriminalu. Ako napadač kasnije obznani kako je spreman učiniti još takvih djela, ukoliko mu se ne ispune neki zahtjevi, riječ je o kibernetskom terorizmu. No, ako je taj napadač još i agent strane protivničkih struktura, tada se djelo može označiti kao kibernetsko ratovanje. Dakle, tek je namjera napadača ono što djelo može okarakterizirati kao kibernetski terorizam, kibernetski rat ili kibernetski kriminal.[37]

Kibernetski terorizam

Kibernetski terorizam označava promišljene, političke motivirane napade izvršene od strane nacionalnih skupina ili prikrivenih čimbenika, odnosno pojedinaca, usmjerene protiv informacijskih ili računalnih sustava, računalnih programa, te podataka, a koji rezultiraju nasiljem nad neborbenim metama. U kolovozu 1997. teroristička skupina *Internet Black Tigers* (IBT), specijalna frakcija Oslobodilačkih tigrova tamilske domovine, nasilne nacionalističke skupine iz Sri Lanke posvećene stvaranju nezavisne države etničkih Tamila, napala je e-mail sustave nekoliko veleposlanstava Sri Lanke diljem svijeta. Preplavljujući te *e-mail* račune s oko 800 emailova na dan, IBT je onesposobio mrežu veleposlanstava skoro dva tjedna. Poslani e-mailovi sadržavali su sljedeću poruku „*We are the Internet Black Tigers and we're doing this to interrupt your communications"*. Skupina je izjavila kako je cilj napada suprotstavljanje promidžbi vlade Sri Lanke.[38]

[37] Ibidem;

[38] Ibidem;

Iako ovaj napad nije prouzročio u bilo kojem smislu velike gubitke, mnogi stručnjaci za terorizam smatraju ga značajnim događajem budućeg razvoja kibernetskog terorizma i terorističkih metoda, a obavještajne zajednice smatraju ga prvim napadom na mreže jedne zemlje. Od tada do danas zabilježeni su brojni slučajevi kibernetskih terorističkih napada.
Kao podvrsta terorizma, kibernetski terorizam koristi informatiku kao oružje, metodu ili metu kako bi se postigao teroristički cilj. Kibernetski terorizam odvija se u kibernetskom prostoru, ali uključuje fizičko uništavanje nekog uređaja, sustava uređaja ili nekog procesa u kojem sudjeluje informatička komponenta. Značajna karakteristika kibernetskog terorizma je prednost da, s obzirom na uloženo, poluči nerazmjeran učinak u uništavanju, uskraćivanju, obmanjivanju, krvarenju, iskorištavanju i remećenju. S obzirom da su teroristi ograničenih sredstava, za pretpostaviti je kako ih kibernetski napadi sve više privlače, jer zahtijevaju manje ljudstva i manje resursa, dopuštaju fizičku odsutnost od mjesta napada, kao i veću mogućnost da napadači ostanu nepoznati, a u kombinaciji s klasičnim terorističkim napadom18 povećavaju učinkovitost terora.[39]

Kibernetski rat

Kibernetski rat (*eng. Cyberwar ili Cyberwarfare*) prema enciklopediji Britannica rat je koji se vodi pomoću računala i mreža koje ih povezuju. Poduzet je od strane država ili drugih od njihove strane angažiranih subjekata protiv drugih država. Kibernetsko ratovanje najčešće se provodi protiv vladinih i vojnih mreža sa svrhom ometanja, uništavanja ili onemogućavanja njihove upotrebe. Kibernetsko ratovanje ne bi se trebalo poistovjetiti s terorističkih korištenjem kibernetskog prostora, niti s kibernetskom špijunažom, a ni skibernetskim kriminalom. Iako se slične taktike koriste u sva četiri oblika djelovanja, pogrešno bi bilo sve ih definirati kao djela kibernetskog ratovanja. Neke države koje su se upustile u kibernetsko ratovanje, mogle bi se također upustiti i u razorne djelatnosti kao što je kibernetska špijunaža, no te djelatnosti same po sebi ne čine kibernetski rat. [40]
Kibernetski rat često se poistovjećuje s informacijskim ratom i informatičkim ratom. Informacijski rat predstavlja postupke poduzete kako bi se postigla informacijska superiornost utjecanjem na informacije protivnika, procese temeljene na informacijama, informacijske

[39] Ibidem;

[40] Ibidem;

sustave i računalne mreže dok se u isto vrijeme brane vlastite informacije, procesi temeljeni na informacijama, informacijski sustavi i računalne mreže. Dakle, može se reći kako je kibernetski rat dio informacijskog rata (ostali dijelovi su primjerice promidžbeni rat, psihološki rat itd.). Informatički rat prema mišljenju autora ovog članka nepotreban je pojam koji unosi zbrku u literaturu. Informatički rat implicira kako je riječ o ratu koji se vrši pomoću informatičke tehnologije, a kako se gotovo svako moderno bojno djelovanje vrši pomoću informatičke tehnologije, besmisleno je govoriti o informatičkom ratu. Primjeri kibernetskog rata su takozvani Prvi mrežni rat (eng. *Web War 1*) u kojem su 2007. u Estoniji *DDOS*-om napadani serveri estonske vlade, ministarstava, medija, banaka i tvrtki, što je rezultiralo isključivanjem tih subjekata s Interneta na određeno vrijeme, te vrlo sličan ruski napad na servere kojim su se koristila brojna vladina tijela, mediji i poslovni subjekti Gruzije, a koji je tekao istovremeno s bojnim djelovanje ruskih snaga spram gruzijskih.[41]

Kibernetski kriminal

Uz prethodna dva pojma postoji i pojam kibernetski kriminal, koji se definira kao kriminal izveden pomoću računalne tehnologije, a u kibernetskom prostoru. Kibernetski kriminal obuhvaća prijevare na polju internetskog bankarstva i prijevare na Internetu s kreditnim karticama, a procjenjuje se kako je s godišnjom stopom rasta od oko 40 posto i s trenutnom zaradom od oko 100 milijardi dolara riječ o najbrže rastućem sektoru globalnog organiziranog kriminala. Potrebno je naglasiti da pod pojam kibernetska kaznena djela treba svrstavati samo kaznena djela kod kojih je uporaba računala ili računalne mreže bitna za biće kaznenog djela, a ne sva kaznena djela u kojima se na neki način kao sredstvo izvršenja pojavljuje računalo s pripadnom perifernom opremom. Tako primjerice kazneno djelo krivotvorenja novca ne spada pod kibernetski kriminal bez obzira što se počinitelj prilikom krivotvorenja novca služio računalnom tehnologijom.[42]

[41] Ibidem;

[42] Ibidem;

4.5. Zakoni, uredbe i državna tijela zadužena za informacijsku sigurnost u Republici Hrvatskoj

Zakoni, uredbe i ostali akti kojima se propisuju okviri, ciljevi i dosezi sigurnosne politike u području kako informacijske tako i kibernetske sigurnosti su:[43]

- Zakon o sigurnosno-obavještajnom sustavu (NN 79/06 i 105/06),
- Zakon o informacijskoj sigurnosti (NN 79/07),
- Zakon o zaštiti osobnih podataka (NN 41/08),
- Zakon o tajnosti podataka (NN 79/07),
- Uredba Vlade RH kojom se propisuju i mjere kibernetske sigurnosti je Uredba o mjerama informacijske sigurnosti (NN 46/08)
- Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti. (NN 108/2015)
- ostali akti državnih tijela (npr. pravilnici, standardni operativni postupci, provedbeni naputci i dr.).

Zakon o informacijskoj sigurnosti (NN 79/07) obuhvatio je slijedeća državna tijela:

- Ured Vijeća za nacionalnu sigurnost
- Zavod za sigurnmost informacijskih sustava
- Nacionalni CERT

Pored nabrojanih državnih tijela iz okvrira Zakona o informacijskoj sigurnosti postoje i druga državna i regionalna tijela koja se bave informacijskom sigurnošću poput Odjela za visokotehnološki kriminal pri Ministarstvu unutarnjih poslova i Regionalno središte za kibernetsku sigurnost unutar Centra za sigurnosnu suradnju-RACVIAC.

[43] Narodne novine (NN; 41/08, 46/08, 79/06, 79/07, 105/06, 108/2015)

Ured Vijeća za nacionalnu sigurnost

Ured Vijeća za nacionalnu sigurnost je središnje državno tijelo za informacijsku sigurnost koje koordinira i usklađuje donošenje i primjenu mjera i standarda informacijske sigurnosti u Republici Hrvatskoj i u razmjeni klasificiranih i neklasificiranih podataka između Republike Hrvatske i stranih zemalja i organizacija.

Ured Vijeća za nacionalnu sigurnost donosi slijedeće pravilnike o standardima; sigurnosne provjere, fizičke sigurnosti, sigurnosti podataka, organizacije i upravljanja područjem sigurnosti informacijskih sustava te sigurnosti poslovne suradnje.

Ured Vijeća za nacionalnu sigurnost (UVNS) trajno usklađuje propisane mjere i standarde informacijske sigurnosti u Republici Hrvatskoj s međunarodnim standardima i preporukama informacijske sigurnosti te sudjeluje u nacionalnoj normizaciji područja informacijske sigurnosti. Surađuje s mjerodavnim institucijama stranih zemalja i organizacija u području informacijske sigurnosti te koordinira međunarodnu suradnju ostalih tijela i pravnih osoba (Zavoda za sigurnost informacijskih sustava i Nacionalnog CERT-a).[44]

Zavod za sigurnost informacijskih sustava

Zavod za sigurnost informacijskih sustava je središnje državno tijelo za tehnička područja sigurnosti informacijskih sustava u tijelima i pravnim osobama državna tijela, tijela jedinica lokalne i područne (regionalne) samo uprave te na pravne osobe s javnim ovlastima, koje u svom djelokrugu koriste klasificirane i neklasificirane podatke.

Tehnička područja sigurnosti informacijskih sustava su:[45]

– standardi sigurnosti informacijskih sustava,
– sigurnosne akreditacije informacijskih sustava,
– upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka,
– koordinacija prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava.

[44]Zakon o informacijskoj sigurnosti, NN (79/07).

[45] Zakon o informacijskoj sigurnosti, NN (79/07)

Zavod za sigurnost informacijskih sustava pravilnicima regulira standarde tehničkih područja sigurnosti informacijskih sustava te trajno usklađuje standarde tehničkih područja sigurnosti informacijskih sustava u Republici Hrvatskoj s međunarodnim standardima i preporukama i sudjeluje u nacionalnoj normizaciji područja sigurnosti informacijskih sustava. Također obavlja poslove sigurnosne akreditacije informacijskih sustava u suradnji s Uredom Vijeća za nacionalnu sigurnost.

Nacionalni CERT *(*eng. *CERT — Computer Emergency Response Team)*

CERT je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj. Zasebna je ustrojstvena jedinica koja se ustrojava u Hrvatskoj akademskoj i istraživačkoj mreži (CARNet).
Usklađuje postupanja u slučaju sigurnosnih računalnih incidenata na javnim informacijskim sustavima nastalih u Republici Hrvatskoj, ili u drugim zemljama i organizacijama, kad su povezani s Republikom Hrvatskom. CERT usklađuje rad tijela koja rade na prevenciji i zaštiti od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj te određuje pravila i načine zajedničkog rada.
CERT i Zavod za sigurnost informacijskih sustava surađuju na prevenciji i zaštiti od računalnih ugroza sigurnosti informacijskih sustava te sudjeluju u izradi preporuka i normi u Republici Hrvatskoj iz područja sigurnosti informacijskih sustava.

Odjel za visokotehnološki kriminalitet pri Ministarstvu unutarnjih poslova

Sustavno analizira, prati i izučava fenomenološki i etiološki aspekt kaznenih djela kibernetičkog (računalnog) kriminaliteta, te predlaže rješenja na planu podizanja razine učinkovitosti rada u suzbijanju kibernetičkog kriminaliteta; neposredno provodi složena kriminalistička istraživanja u području kaznenih djela počinjenih na štetu i pomoću računalnih sustava i mreža; obavlja forenzičku analizu i nadzor interneta; pruža specijaliziranu potporu drugim ustrojstvenim jedinicama policije; surađuje s drugim ustrojstvenim jedinicama Ministarstva, tijelima državne uprave i pravnim osobama, policijama drugih zemalja i međunarodnim institucijama u svom djelokrugu rada; sudjeluje u planiranju i izradi programa obuke policijskih službenika u čijem je djelokrugu rada problematika kibernetičkog

kriminaliteta; sudjeluje u izradi normativnih akata, izvješća i drugih stručnih materijala iz područja kibernetičkog kriminaliteta te obavlja i druge poslove iz svoga djelokruga rada.[46]

RACVIAC - Centar za sigurnosnu suradnju

RACVIAC – Centar za sigurnosnu suradnju je međunarodna, nezavisna, neprofitna i akademska organizacija u vlasništvu zemalja Jugoistočne Europe osnovana sa ciljem promicanja dijaloga i suradnje u području sigurnosti. RACVIAC predstavlja snažan instrument za jačanje stabilnosti i sigurnosti država regije a ujedno i moguću platformu za prenošenje znanja i iskustava u druga područja. Posebnost RACVIAC-a jest što je u vlasništvu zemalja JI Europe gdje same članice raspravljaju o sigurnosnim pitanjima od zajedničkog interesa.[47]
Inicijativu za osnivanje RACVIAC-a sa sjedištem u Republici Hrvatskoj pokrenula je 1999. godine SR Njemačka. Sporazum o osnivanju RACVIAC-a sklopljen je 8. ožujka 2001. godine između Republike Hrvatske i Savezne Republike Njemačke u okviru Pakta o stabilnosti. RACVIAC je počeo djelovati kao multinacionalno regionalno središte za pomoć u provedbi sporazuma o nadzoru naoružanja u zemljama Jugoistočne Europe. Uzimajući u obzir neprestani razvoj i promjene u sigurnosnom okruženju u području jugoistočne Europe, gašenje Pakta o stabilnosti, te jačanje „regionalnog vlasništva“, zainteresirane države Procesa suradnje u jugoistočnoj Europi (SEECP-a) pristupile su reorganizaciji i preustroju RACVIAC-a.
Ugovor o RACVIAC- Centru za sigurnosnu suradnju potpisan je 14. travnja 2010 g. od strane Republike Albanije, Bosne i Hercegovine, Crne Gore, Helenske Republike, Republike Hrvatske, Republike Makedonije, Republike Srbije, Republike Turske i Rumunjske. Ugovor je stupio na snagu 1. prosinca 2011. g. Prema Ugovoru članice RACVIAC-a imaju obvezu sekundiranja osoblja, plaćanja članarine i jedine su nadležne za donošenje odluka. Pridružene članice najčešće sudjeluju u financiranju pojedinih projekata i programa. Republika Hrvatska ima veliki interes za punom i aktivnom podrškom RACVIAC-u, s obzirom da je sjedište ove međunarodne organizacije u Zagrebu, u Rakitju, a istovremeno područje djelovanja RACVIAC-a – stabilnost i sigurnost u Jugoistočnoj Europi,jedan je od vanjsko političkih prioriteta. Republika Hrvatska također vidi suradnju zemalja članica u okviru RACVIAC-

[46] Uredba o unutarnjem ustrojstvu Ministarstva unutarnjih poslova Republike Hrvatske, (NN 70/2012)

[47]Web stranice Ministarstva vanjskih i europskih poslova: http://www.mvep.hr/hr/vanjska-politika/multilateralni-odnosi0/medunarodna-sigurnost/racviac/ (31.10.2017)

a kao dodanu vrijednost uspješnom ostvarivanju reformi i razvitka zemalja članica ka ispunjavanju visokih kriterija za članstvo u euro-atlantskim integracijama.
Od listopada 2015. godine direktor RACVIAC-a je veleposlanik Haydar Berk (Turska). Glavno težište djelovanja RACVIAC-a su reforma sigurnosnog sektora, međunarodna suradnja glede bržeg integriranja zemalja Jugoistočne Europe u euroatlantske integracije te sigurnosna suradnja u području kontrole naoružanja.[48]

Zemlje članice: Albanija, Bosna i Hercegovina, Crna Gora, Hrvatska, Makedonija, Srbija, Turska i Rumunjska.
Pridružene članice: Austrija, Republika Češka, Danska, Francuska, Njemačka, Mađarska, Italija, Nizozemska, Norveška, Rusija, Slovenija, Španjolska, Švedska i Ujedinjeno Kraljevstvo.
Promatrači: Kanada, Moldavija, Poljska, Slovačka, Ukrajina, Sjedinjene Američke Države i Grčka.

[48] Ibidem:

5. NORME SERIJE ISO 27000

Norme iz serije ISO 27000 izrađene su tako da svaka od normi daje naglasak na nešto. U daljnjem tekstu nabrojane su norme od ISO 27001 do ISO 27006 i u jednoj rečenici objašnjen je naglasak pojedine norme:[49]

- **ISO 27001** služi za postavljanje temelja informacijske sigurnosti i određivanje njezinih okvira.
- **ISO 27002** služi za implementaciju sigurnosnih mjera, sadrži najbolje prakse u uvođenju norme.
- **ISO 27003** pruža upute za implementaciju kao pomoć osobama koje implementiraju ISO 27000 standarde. U osnovi se bazira na smjernicama iz ISO 27001 standarda, te pruža vodstvo sve do pokretanja ISMS projekta.
- **ISO 27004** služi da pomogne organizacijama mjeriti, izvještavati i na temelju istoga sistematski poboljšavati kvalitetu ISMS.
- **ISO 27005** služi za provedbu procjene rizika.
- **ISO 27006** je akreditacijski standard koji vodi certificiranje kroz formalni proces certifikacije ISMS organizacija prema ISO 27001 standardu. U istome su navedene sve potrebe i upute kako izvesti certifikaciju i koje uvjete organizacija mora zadovoljiti.

5.1. ISO/IEC 27001

Prije nastajanja ISO normi, postojala je BS 7799 norma (nastala pod okriljem British Standard Institute- BSI). Prvi put je izišla kao kodeks dobre prakse 1995.g. Podijeljena na dva dijela 1999. godine na BS 7799-1 i BS 7799-2. Nekoliko godina kasnije, normu BS 7799-1 preuzima ISO (Međunarodna organizacija za standardizaciju) i izdaje ju pod imenom ISO/IEC 17799. Kasnije je norma BS 7799-2 izdana kao ISO/IEC 27001:2005 u kojoj su opisani pojedini elementi sustava upravljanja sigurnošću informacija. Norma je napisana u obliku zahtjeva, koje sustav treba ispunjavati, a omogućava ocjenjivanje bilo interno ili vanjsko, od neovisne certifikacijske institucije.[50]

[49] Kostanjevec A., i dr.. Sigurnost informacijskih sustava verzija 01012014, FOI Varaždin 2014. str.28.

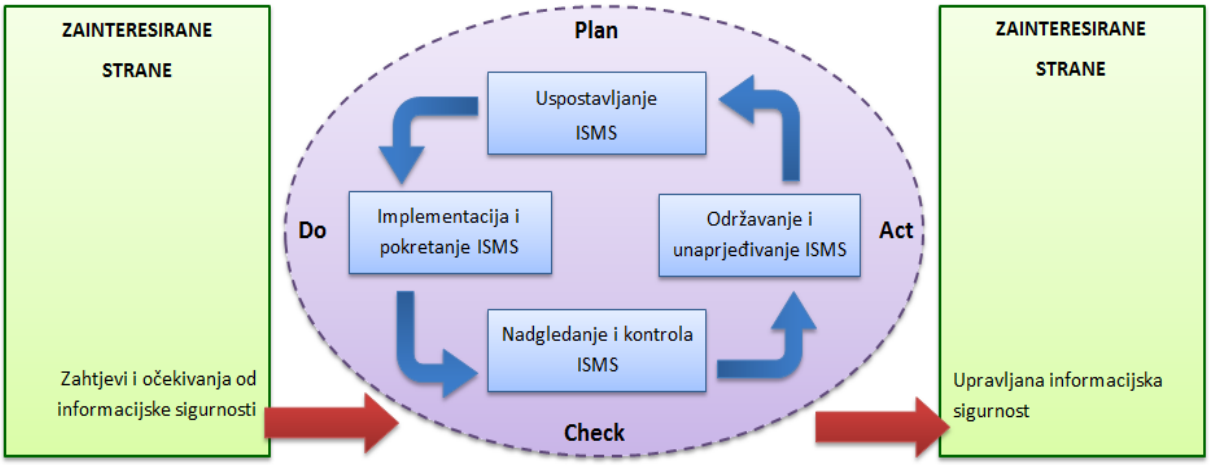
[50] Ibidem; str.17

Posljednja verzija norme ISO/IEC 27001 objavljena je u rujnu 2013. godine te propisuje ukupno 114 sigurnosnih kontrola koje su specificirane u 7 klauzula i 18 skupina u prilogu A (*Annex A*).[51]

5.1.1. Procesni pristup

ISO 27001 usvaja procesni pristup za:[52] uspostavljanje, implementaciju, rad, nadziranje, provjeru, održavanje i unaprjeđivanje organizacijskog ISMS-a. Organizacija treba identificirati i upravljati mnogim aktivnostima ukoliko želi učinkovito funkcionirati. Bitno je naglasiti kako ova međunarodna norma usvaja **PDCA model**.

Slika 7. PDCA model



Izvor: Kostanjevec A. i dr.. Sigurnost informacijskih sustava verzija 01012014, FOI Varaždin 2014. str.17.

Slika prikazuje uzimanje zahtjeva za informacijsku sigurnost i očekivanja zainteresiranih strana, kao ulaznu komponentu, te kroz neophodne procese stvara rezultate informacijske sigurnosti koji odgovaraju tim zahtjevima i očekivanjima, kao izlaznu komponentu.
PDCA model je skraćeni naziv za „Plan-Do-Check-Act“ model i primjenjen je u oblikovanju svih ISMS procesa.

[51] Krakar Zdravko i suradnici; Korporativna informacijska sigurnost, Fakultet organizacije i informatike Varaždin 2014. Str.139.

[52] Kostanjevec A.,Bartošek G i dr.. Sigurnost informacijskih sustava verzija 01012014, FOI Varaždin 2014. str.17.

Opis PDCA modela

- ***Plan*** (uspostaviti ISMS) Uspostaviti ISMS politiku, ciljeve, procese i procedure važne za upravljanje rizikom i poboljšanje informacijske sigurnosti kako bi dali rezultate u skladu s ukupnom politikom i ciljevima organizacije.
- ***Do*** (implementirati i izvršavati ISMS). Implementirati i izvršavati ISMS politiku, kontrole, procese i procedure.
- ***Check*** (nadgledati i provjeravati ISMS). Procijeniti i gdje je primjenjivo, mjeriti izvršavanje procesa u odnosu na ISMS politiku, ciljeve i praktično iskustvo, te izvještavati upravu o rezultatima radi provjere.
- ***Act*** (održavati i poboljšavati ISMS). Poduzeti korektivne i preventivne akcije zasnivane na rezultatima interne ISMS prosudbe (audita) i provjere uprave ili ostalim bitnim informacijama kako bi se postiglo stalno poboljšanje ISMS-a.

5.1.2. Terminologija

Za potrebe ISO 27001 definiraju se i primjenjuju sljedeći nazivi i definicije:[53]

Imovina - sve što predstavlja vrijednost za organizaciju.
Dostupnost - osobina dostupnosti i upotrebljivosti imovine na zahtjev ovlaštenog entiteta.
Povjerljivost - osobina da informacija nije učinjena dostupnom ili otkrivena neovlaštenim osobama, entitetima ili procesima.
Informacijska sigurnost - očuvanje povjerljivosti, integriteta i dostupnosti informacije uključiti se mogu i druge osobine kao što su vjerodostojnost, odgovornost, neporecivost i pouzdanost.
Sigurnosni događaj - prepoznatljiv slučaj stanja sustava, usluge ili mreže koji upućuje na moguću povredu politike informacijske sigurnosti ili neuspjeh zaštite ili do tada nepoznate okolnosti koje mogu biti važne za sigurnost.
Sigurnosni incident - jedan ili više neželjenih ili neočekivanih sigurnosnih događaja koji imaju značajnu vjerojatnost ugrožavanja poslovnih aktivnosti i informacijske sigurnosti.

[53] Ibidem;

Sustav upravljanja informacijskom sigurnošću (ISMS) - dio cjelokupnog sustava upravljanja, temeljen na pristupu sa stane poslovnih rizika, kako bi uspostavio, implementirao, nadzirao, provjeravao, održavao i unapređivao informacijsku sigurnost.

Integritet - osobina očuvanja autentičnosti i cjelovitosti imovine.

Rezidualni rizik - preostali rizik nakon obrade rizika.

Prihvaćanje rizika - odlika da se rizik prihvati.

Analiza rizika - sustavna uporaba informacija za određivanje izvora i procjenu rizika.

Procjena rizika - cjelokupan proces analize i njegovo vrednovanje.

Vrednovanje rizika - proces usporedbe procijenjenog rizika sa danim kriterijima, kako bi se ustanovio značaj rizika.

Upravljanje rizikom - usklađene aktivnosti za usmjeravanje i kontrolu organizacije u smislu rizika.

Obrada rizika - proces odabira i primjene mjera za promjenu rizika.

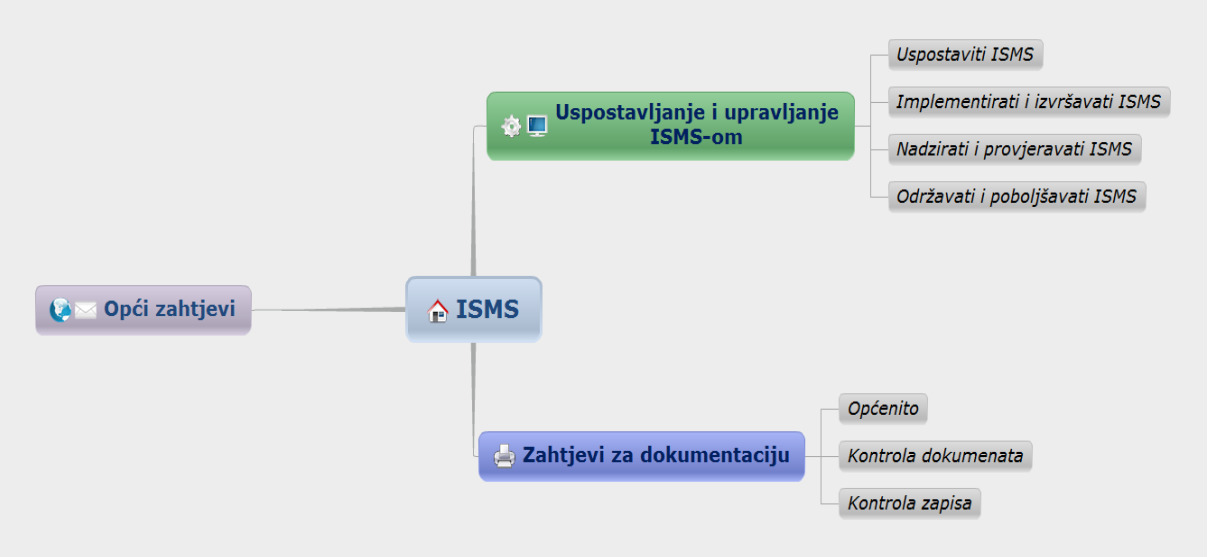
Izjava o primjenjivosti - dokumentirana izjava koja opisuje ciljeve kontrola i kontrole koje su relevantne i primjenjive na ISMS organizacije.

5.1.3. ISMS

ISMS (eng. *Information Security Management Systems*) je sustav upravljanja informacijskom sigurnošću. Prema ISO 27001 normi, pruža sustavan pristup upravljanju osjetljivim informacijama kako bi ih zaštitio i obuhvaća sve što je unutar organizacije, a tiče se procesa, informacijske imovine i zaposlenika. ISMS također možemo nazvati „sredstvo“ kojim uprava neke organizacije prati i nadzire sigurnost informacijskog sustava. Za izgradnju sustava upravljanja informacijskom sigurnošću potreban je PDCA model (spomenut u prethodnom poglavlju), koji se kontinuirano provodi. Izgradnja samog ISMS-a je iterativni proces koji se neprestano nadograđuje i poboljšava.[54]

[54] Ibidem; str.20.

Slika 8. Koraci u izgradnji ISMS-a



Izvor: Kostanjevec A. i dr.. Sigurnost informacijskih sustava verzija 01012014, FOI Varaždin 2014. str.20.

5.1.4. Opći zahtjevi

Što se tiče općih zahtjeva u organizaciji je važno:[55] upostaviti, implementirati, izvršavati, nadzirati, održavati i poboljšavati dokumentirani ISMS unutar konteksta cjelokupnih poslovnih aktivnosti organizacije i rizika s kojima se ona suočava.

5.1.5. Uspostavljanje i upravljanje ISMS-om

Što se tiče uspostavljanja i upravljanja ISMS-om, ono se dijeli na četiri podgrupe:[56]

1. Uspostaviti ISMS
2. Implementirati i izvršavati ISMS
3. Nadzirati i provjeravati ISMS i
4. Održavati i poboljšavati ISMS

[55] Ibidem;

[56] Ibidem;

1. Uspostaviti ISMS

Da bi se uopće uspostavio ISMS, organizacija mora poduzeti nekoliko koraka, a to su:

a) Određivanje opsega i granica ISMS-a

b) Definiranje politike ISMS-a

c) Definiranje pristupa organizacije procjeni rizika

d) Identifikacija rizika

e) Analiza i vrednovanje rizika

f) Identifikacija i vrednovanje opcija za obradu rizika

g) Odabir ciljeva kontrola i kontrola za obradu rizika

h) Dobivanje odobrenja uprave za predložene rezidualne rizike

i) Dobivanje ovlaštenja uprave za implementaciju i izvršavanje ISMS-a

j) Priprema Izjave o primjenjivosti

2. Implementirati i izvršavati ISMS

Nakon što su se ispunili svi uvjeti za uspostavu ISMS-a, sljedi korak implementacije i izvršavanja ISMS-a:

a) Formulacija plana za obradu rizika

b) Implementacija plana za obradu rizika

c) Implementacija odabranih kontrola kako bi se zadovoljili ciljevi kontrola

d) Određivanje načina mjerenja učinkovitosti odabranih kontrola ili grupa kontrola

e) Implementacija programa obuke i podizanja svijesti o informacijskoj sigurnosti

f) Upravljanje izvršavanjem ISMS-a

g) Upravljanje resursima za ISMS

h) Implementacija procedure i drugih kontrola sposobnih za omogućavanje pravovremene detekcije sigurnosnih događaja i odgovor na sigurnosne incidente

3. Nadzirati i provjeravati ISMS

Za provođenje implementacije i izvršavanja ISMS-a može se reći da je posljednji korak u uspostavi ISMS-a. Nakon što organizacija uspješno provede cjelokupnu uspostavu ISMS-a, na red dolazi kontrola, odnosno nadziranje i provjera ISMS-a, a koja obuhvaća sljedeće:

a) Izvršavanje procedure nadzora i provjere, te ostale kontrole

b) Izvođenje redovite provjere učinkovitosti ISMS-a
c) Mjerenje učinkovitosti kontrola (svrha: provjera da li su sigurnosni zahtjevi zadovoljeni)
d) Provjeravanje procjene rizika u planiranim intervalima
e) Provođenje interne prosudbe u planiranim intervalima
f) Provođenje provjere ISMS-a od strane uprave na redovnoj bazi
g) Nadopunjavanje sigurnosnih planova kako bi se u obzir uzeli rezultati aktivnosti za nadzor i provjeru
h) Bilježenje akcija i događaja koji bi mogli imati učinak na učinkovitosti ili izvođenju ISMS- a

4. Održavati i poboljšavati ISMS

Posljednji korak koji organizacija mora redovito provoditi, a tiče se dijela upravljanja ISMS-om je održavanje i poboljšavanje ISMS-a, koje se provodi kroz par koraka:
a) Implementacija uočenih poboljšanja ISMS-a
b) Poduzimanje odgovarajućih korektivnih i preventivnih akcija
c) Obavještavanje svih zainteresiranih strana o aktivnostima i poboljšanjima
d) Osiguranje da poboljšanja postignu njihove namjeravane ciljeve
Tek nakon ovih dugotrajnih procesa, može se reći da je ISMS, ne samo uspješno postavljen, već i održavan od strane organizacije.

5.1.6. Zahtjevi za dokumentaciju

Na slici 8. može se vidjeti što sve obuhvaćaju *Zahtjevi za dokumentaciju*.

Zahtjevi za dokumentaciju dijele se u 3 podgrupe:[57]
1. Općeniti zahtjevi
2. Kontrola dokumenata
3. Kontrola zapisa.

1. Općeniti zahtjevi

Općenito, dokumentacija mora sadržavati zapise o odlukama uprave, zatim osiguravati sljedivost postupaka do odluka uprave i politika, te na kraju osigurati da se zapisani rezultati

[57] Ibidem;

mogu ponovno proizvesti. Ukratko, sada će biti nabrojano što sve ISMS dokumentacija mora sadržavati:

a) Dokumentirane izjave ISMS politike i ciljeva

b) Opseg ISMS-a

c) Procedure i kontrole koje podupiru ISMS

d) Opis metodologije procjene rizika

e) Izvještaj procjene rizika

f) Plan obrade rizika

g) Organizaciji potrebne dokumentirane procedure za učinkovito planiranje, rad i kontrolu njenih procesa informacijske sigurnosti

h) Zapise zahtijevane ovom međunarodnom normom

i) Izjavu o primjenjivosti

2. Kontrola dokumenata

Dokumenti moraju biti zaštićeni i kontrolirani. Također, mora biti uspostavljena procedura koja će odrediti akcije uprave potrebne kako bi se:

a) Odobrila adekvatnost dokumenata prije izdavanja

b) Pregledali i dopunili dokumenti i ponovo odobrili

c) Osiguralo da se identificirane izmjene i status trenutne revizije dokumenata

d) Osiguralo da su relevantne verzije primjenjivih dokumenata dostupne na mjestu upotrebe

e) Osiguralo da dokumenti ostanu čitki i lako prepoznatljivi

f) Osiguralo da su dokumenti dostupni onima koji ih trebaju

g) Osiguralo da su identificirani dokumenti vanjskog porijekla

h) Osiguralo da je distribucija dokumenata kontrolirana

i) Spriječilo nenamjernu upotrebu zastarjelih dokumenata

j) Ukoliko su iz bilo kod razloga sačuvanima, dokumentima dodijelilo odgovarajuću identifikaciju

3. Kontrola zapisa

Moraju se uspostaviti i održavati zapisi koji pružaju dokaze o usklađenosti sa zahtjevima i učinkovitom radu ISMS-a. Oni moraju biti zaštićeni i kontrolirani. Zapisi moraju ostati čitki, lako prepoznatljivi i dostupni. Kontrole moraju biti dokumentirane i implementirane.

5.1.7. Odgovornost uprave

Što se tiče odgovornosti uprave, dvije su stvari na koje se odgovornost uprave dijeli, a to su: [58]
1. Opredjeljenje uprave i
2. Upravljanje sredstvima

Opredjeljenje uprave
Uprava mora pružiti dokaz svoje opredjeljenosti uspostavi, implementaciji, izvršavanju, nadziranju, provjeri, održavanju i poboljšanju ISMS-a. To može učiniti kroz veći broj uvjeta, a neki od njih su:
- Uspostavljanje ISMS politike
- Osiguravanje da su ciljevi i planovi ISMS-a uspostavljeni
- Odlučivanje o kriteriju za prihvaćanje rizika i prihvatljivim razinama rizika
- Osiguranje provođenja internih prosudbi (audita) ISMS-a
- Provođenjem provjera ISMS-a od strane uprave

Upravljanje sredstvima
Upravljanje sredstvima dijeli se na:
- Dodjeljivanje sredstava
- Obučavanje, razina svijesti i sposobnosti

5.1.8. Interne prosudbe (auditi) ISMS-a

Interne prosudbe, odnosno auditi moraju se provoditi u planiranim intervalima, kako bi se ustanovilo da ciljevi kontrola, kontrole, te procesi i procedure njenog ISMS-a udovoljavaju zahtjevima ove međunarodne norme i identificiranim zahtjevima informacijske sigurnosti, te učinkovito implementirani i održavani i izvršavaju se kako se od njih očekuje. Dokumentiranom procedurom moraju također biti definirani odgovornosti i zahtjevi za planiranje i provođenje prosudbi.[59]

[58] Ibidem;

[59] Ibidem;

Provjera ISMS-a od strane uprave

Kao što se provode interne prosudbe u planiranim intervalima od strane organizacije, također se i provjera organizacijskog ISMS-a mora održavati i to minimalno jednom godišnje. Provjeravanje ISMS-a osigurava njegovu stalnu podobnost, primjerenost i učinkovitost. Za provjeru ISMS-a bitni su ulazni podaci, te na kraju i sami rezultati provjere. U daljnjem tekstu ukratko su nabrojani ulazni podaci i rezultati provjere.[60]

- **Ulazni podaci za provjeru** – podaci koje je potrebno dostaviti upravi za potrebe provjere sadržavaju:

- Rezultate prosudbi i provjera ISMS-a
- Povratne informacije zainteresiranih strana
- Status preventivnih i korektivnih akcija
- Rezultate mjerenja učinkovitosti
- Naknadne akcije iz prethodnih provjera uprave
- Preporuke za poboljšanje

- **Rezultati provjere** uprave moraju sadržavati sve odluke i akcije vezane uz sljedeće:

- Poboljšanje učinkovitosti ISMS-a
- Ažuriranje procjene rizika i plana obrade rizika
- Izmjene procedura i kontrola
- Potrebe za sredstvima
- Poboljšanja načina mjerenja učinkovitosti kontrola

5.1.9. Poboljšanje ISMS-a

Poboljšanje ISMS-a dijeli se na 3 skupine:[61]

1. Stalno poboljšanje
2. Korektivne akcije i
3. Preventivne akcije

[60] Ibidem;

[61] Ibidem, str. 26.

Kada se govori o **stalnom poboljšanju**, onda se misli na to da organizacija mora konstantno poboljšavati učinkovitost ISMS-a. Poboljšavanje učinkovitosti ISMS-a odvija se kroz uporabu politike informacijske sigurnosti, ciljeva informacijske sigurnosti, rezultata prosudbi i slično. Osim stalnog poboljšavanja, moraju se poduzimati i **korektivne akcije** kako bi se uklonili uzroci nesukladnosti sa ISMS zahtjevima, te se mora provoditi dokumentirana procedura za korektivnu akciju, koja pak mora definirati zahtjeve za:[62]

- Identificiranje nesukladnosti
- Ustanovljavanje uzroka nesukladnosti
- Ustanovljavanje i implementiranje potrebne korektivne akcije
- Provjeravanje poduzete korektivne akcije

Na kraju, pored stalnog poboljšanja i korektivnih akcija, postoje i **preventivne akcije**, što podrazumijeva da organizacija mora odrediti akciju za uklanjanje uzroka koji može uzrokovati potencijalne nesukladnosti sa ISMS zahtjevima. Organizacija mora identificirati promijenjene rizike i identificirati zahtjeve za preventivnom akcijom s pažnjom usmjerenom na znatno promijenjene rizike.

5.1.10. Koraci za implementaciju norme ISO/IEC 27001

Za implementaciju norme ISO/IEC 27001 potrebito je uspostaviti i dokumentirati područje upravljanja sigurnošću organizacije. Potrebno je definirati opseg ISMS-a čije granice treba definirati u skladu s karakteristikama organizacije, njene lokacije, vrijednosti i tehnologijom. Implementacija norme ISO/IEC 27001 provodi se kroz 8 glavnih koraka koje je potrebno slijedno provoditi.[63]

1. Započinjanje projekta**.**

Za započinjanje projekta potrebno je osigurati potporu višeg menadžmenta i odabrati i obučiti članove inicijalnog projektnog tima. U ovom koraku nužno je usvojiti sigurnosnu politiku.

[62] Ibidem;

[63] Bogati Javor; Praktični menadžment; Vol.2. No.2. Prosinac 2011. Visoka škola za menadžment u turizmu i informatici u Virovitici, Str. 112. – 117.

2. Definiranje ISMS-*a*.

Za implementaciju norme ISO/IEC 27001 potrebito je uspostaviti i dokumentirati područje upravljanja sigurnošću organizacije. Potrebno je definirati opseg ISMS-a čije granice treba definirati u skladu s karakteristikama organizacije, njene lokacije, vrijednosti i tehnologijom.

Inicijalni projektni tim mora definirati okvir upravljanja informacijskom sigurnošću kako bi se fokusirao na ključne elemente. Sigurnosni opseg može pokriti pojedine odjele organizacije ili cjelokupnu organizaciju. Kod utvrđivanja ISMS-a potrebno je jasno utvrditi:[64]

- Cilj i svrhu informacijskog sustava;
- Opseg;
- Granice i ograničenja;
- Međusklopove;
- Ovisnosti;
- Izuzeća i opravdanja;
- Strateški kontekst;
- Organizacijski kontekst.

3. Procjena rizika**.**

Potrebno je provesti početnu procjenu sukladnosti statusa sustava za upravljanje informacijskom sigurnošću u okviru kontrola, procesa i procedura zahtijevanih normom ISO 27001.

Idući korak je utvrđivanje imovine i njenog vrednovanja, odnosno utvrđivanje kritičnih i povjerljivih podataka.

Nakon toga potrebno je utvrditi i vrednovati prateću i potpornu imovinu (kvantitativno i/ili kvalitativno), a to je neopipljiva imovina kojom se rukuje i komunicira, koja se obrađuje, pohranjuje, ispisuje, te procesuira i odlaže kroz opipljiva sredstva.

Na kraju se provodi utvrđivanje i vrednovanje prijetnji i ranjivosti, gdje je od velike važnosti prepoznati slabosti svakog dijela imovine koji podržava kritične informacije organizacije. Takve su slabosti ranjive na prijetnje i zbog toga mogu imati negativan učinak na podatke i informacije.

[64] Ibidem;

Općenito, rizik kao pojam predstavlja kombinaciju vjerojatnosti nekog događaja i utjecaja, odnosno (negativne) posljedice tog događaja u slučaju realizacije prijetnji koje iskorištavaju neku od ranjivosti.

Kad se govori o informacijskoj sigurnosti, rizik (R) za pojedini resurs procjenjuje se procjenom njegove vrijednosti (*engl. asset value* – AV), ranjivosti tog resursa (*engl. vulnerability* – V), prijetnji koje mogu iskoristiti te ranjivosti (*engl. threat* – T), vjerojatnosti ostvarenja prijetnji (*engl. probability* – P) i posljedicama (*engl. impact* – I) koje se mogu dogoditi ukoliko se određena prijetnja ostvari. Dakle, matematički rizik predstavlja funkciju navedenih varijabli.

$R = f\,(AV,V,T,P,I\,)$

Također, da bi se rezultati procjene rizika mogli smatrati valjanima, sam proces mora zadovoljiti sljedeće kriterije:[65]

- jednoznačnost;
- objektivnost;
- pouzdanost i
- repetabilnost.

4. Upravljanje rizikom**.**

Prilikom upravljanja rizikom treba izabrati neku od sljedećih opcija:[66]

- smanjenje rizika;
- prihvaćanje rizika;
- izbjegavanje rizika;
- prijenos rizika.

Nakon odabira opcije potrebito je postaviti ciljeve i implementirati kontrole te izraditi plan upravljanja rizikom koji treba sadržavati: zadatke i odgovornosti, imena sudionika, prioritet uprave i drugo. Plan upravljanja rizikom mora se provesti i treba ga nazirati definiranim kontrolama.

[65] Ibidem;

[66] Ibidem,

5. Obuka i osvješćivanje.

Organizacija mora osigurati da su svi članovi kojima je dodijeljena odgovornost pri uspostavi ISMS-a osposobljeni za obavljanje svojih zadataka. Uzimajući tu činjenicu u obzir organizacija mora:[67]

- Utvrditi potrebne vještine za rad na informacijskoj sigurnosti;
- Pružiti odgovarajuću obuku i, po potrebi, zaposliti iskusno osoblje za ovaj zadatak;
- Ocijeniti učinkovitost pružene obuke i poduzetih aktivnosti;
- Čuvati zapis o programu obuke za svakog zaposlenika, uključujući i njihove vještine, iskustvo i kvalifikacije.

6. Priprema za reviziju.

Prije same revizije mora biti izrađena – Izjava o primjenjivosti.

Taj dokument pruža opravdanja o primjenjivosti ili neprimjenjivosti svake od ISO/IEC 27001 kontrola ISMS-a za koju se vrši revizija. Dokument također uključuje, gdje je primjenjivo, te trenutni implementacijski status svake kontrole. Ukratko, u tom su dokumentu objašnjeni ciljevi, odabrane kontrole i razlozi za njihov odabir, kao i razlozi izuzimanja bilo koje od kontrola propisanih normom ISO/IEC 27001.

7. Revizija**.**

Revizija se provodi kroz dva dijela, a to su revizija dokumentacije i revizija implementacije.

8. Neprekidno osvješćivanje.

Nakon što je implementirano upravljanje sigurnošću informacijskim sustavom, važno je redovito provjeravati i unaprjeđivati upravljački okvir.

[67] Ibidem;

5.1.11. Prednosti ISO 27001 certificiranja

Prednosti certificiranja prema ISO 27001 najbolje je predočio australski web portal CRN (ComputerReseller News) 2009.godine sa ovih 10 razloga:[68]

1. ISO 27001 je internacionalno prepoznat, pa će i iskustvo organizacije biti.
2. Najbolja praksa; odvajanje onih sa stvarnim iskustvom od onih koji samo razmišljaju o tome na način da se profitira od iskustva drugih.
3. Baziran na riziku; gleda što organizacija treba, te ne nameće određene standarde; pravovremeni, pravedni i isplativ savjet.
4. Standard za upravljanje, a ne tehnički standard; daje model upravi koja tada mora pokazati svoje vještine donošenja odluka.
5. Holistički; razmatra sve aspekte informacijske sigurnosti, ne samo tehničke mjere, demonstrira dubinu i širinu.
6. Organizacije mogu biti nezavisno certificirane; daje vanjski nezavisni pogled na poslove o sigurnosti u organizaciji.
7. Daje način kako držati rizike pod kontrolom, dopuštajući redovit pregled i objektivnu analizu rizika.
8. Daje proces za praćenje sigurnosti i napretka; mogućnost dokazivanja koristi od sigurnosti i ulaganja u sigurnost.
9. Komplementaran je sa drugim standardima, poput ISO 9001, ISO 14001 i ISO 20001.
10. Svaka organizacija sa ISO 27001 certifikatom je izjavila da je popravila upravljanje sigurnošću u organizaciji.

[68] CRN, australski web portal; https://www.crn.com.au/news/10-reasons-why-iso-27001-makes-a-better-is-security-professional-152262 (30.10.2017.)

5.2. Aplikativni primjer uvođenja norme ISO 27001 u organizaciju

Kao aplikativni primjer uvođenja norme ISO 27001 navesti će se fiktivni primjer uvođenja u jedan dio organizacije, Županijski centar 112 (ŽC 112) pri Državnoj upravi za zaštitu i spašavanje Republike Hrvatske (DUZS).

Prvi, odnosno može se nazvati nulti korak je predanost uprave odnosno top menadžmenta implementaciji norme ISO 27001 u cijelu organizaciju. Nakon toga oformljena je radna skupina za uvođenje norme ISO 27001 u organizaciju te su članovi radne skupine upućeni na edukaciju za interne auditore norme ISO 27001 pri certifikacijskom tijelu koje će osim edukacije provesti i certifikaciju organizacije prema navedenoj normi. Razvoj ISMS sustava započinje definiranjem opsega ISMS-a u što spada cjelokupna Državna uprava za zaštitu i spašavanje (DUZS). U ovoj cjelini opisati će se uvođenje norme ISO 27001 u jedan manji dio DUZS-a odnosno ŽC112 u Zagrebu. ŽC 112 već ima primjenjene određene sigurnosne kontrole poput: kontrole pristupa (u ŽC 112 može se ući samo kroz protuprovalna vrata koja se otvaraju pomoću lozinke), autentifikacije korisnika u sustav - svaki djelatnik mora se *ulogirati* na sustav preko računala na svom radnom mjestu, a sva računala povezana su u računalnu mrežu preko servera na kojem su instalirani programi za antivirusnu zaštitu, a informatičari iz Odjela za informacijsku i komunikacijsku tehnologiju zaduženi su za administraciju servera te odnose sa vanjskim pružateljima usluga administracije te nadogradnje servera. Informacijska sigurnost je poglavlje spomenuto i obrađeno u dokumentu „Naputak o radu dežurne smjene“ što svakom djelatniku ŽC 112 predstavlja obavezu pridržavati se propisanih pravila koja su u naputku obrađena. Naputak o radu dežurne smjene predstavlja također svojevrsni dokument politike informacijske sigurnosti.

Radna skupina odnosno interni auditori procjenjuju trenutačno stanje i obavljaju razgovore sa vlasnicima procesa. U vlasnike procesa spadaju svi djelatnici ŽC 112, uključujući operatere-analitičare, voditelje dežurnih smjena te voditelja ŽC 112 (koji je i operativni menadžer). Ovdje je uloga operativnog menadžera vrlo bitna, treba motivirati djelatnike za sudjelovanje u implementaciji norme, stimulirati svako poželjno, a destimulirati svako nepoželjno ponašanje. Kao primjer toga naveo bih zaposlenike koji aktivno pomažu internim auditorima u uvođenju norme, daju sugestije i brinu se da internim auditorima boravak i rad u ŽC 112 bude što produktivniji i ugodniji, takve zaposlenike treba pohvaliti te njihovo ponašanje tijekom internog audita operativni menadžer treba uzeti u obzir na kraju godine kada svi djelatnici dobivaju

ocjene za svoj rad (državni službenici na kraju svake godine dobivaju ocjene za svoj rad koje imaju utjecaja na napredovanje, dane godišnjeg odmora i dr.).

Interni auditori započinju sa indentifikacijom i klasifikacijom informacijske imovine, koju čine sve informacije u papirnatom i elektroničkom obliku, računala (*hardver i softver*), medije na kojima je informacijska imovina pohranjena, telekomunikacijska oprema (telefoni, uređaji za radio komunikaciju i dr.), cjelokupni sustav za uzbunjivanje stanovništva, sefovi, namještaj u kojima i na kojima se nalazi informacijska imovina te naravno ono najbitnije, ljudi odnosno djelatnici koji sa istom imovinom rade i njome u operativnom radu upravljaju. Klasifikacija informacijske imovine radi se prema kriterijima *(CIA)*, što podrazumjeva očuvanje povjerljivosti, integriteta i raspoloživosti informacijske imovine. Najbolje je da klasifikaciju imovine provodi osoba koja dobro poznaje sustav odnosno organizaciju, tako da u slučaju klasifikacije informacijske imovine u ŽC 112 istu provodi interni auditor koji je zaposlenik ŽC 112 u suradnji sa operativnim menadžerom – voditeljem ŽC 112.

Temeljem provedene klasifikacije, identificira se kritična imovina za koju je nužno provesti procjenu rizika i prepoznati kontrole, kojima bi se ti rizici umanjili. Postoji niz unaprijed definiranih metodologija za procjenu rizika poput:[69] *CRAMM, OCTAVE i FMEA*. Norma ISO 27001 ne preferira niti jednu od njih, a kao dobra polazna osnova može se koristiti norma ISO 27005:2011 koja pruža smjernice za upravljanje rizicima i podržavajući zahtjeve sustava upravljanja informacijskom sigurnošću prema normi ISO 27001 te omogućava detaljnije pristupe procjeni rizika informacijske sigurnosti od procjene rizika visoke razine do raznih metoda i tehnika. U slučaju procjene rizika angažira se vanjska firma odnosno poduzeće koje se time bavi dugi niz godina. Razlog tome je što interni auditori pored svog redovnog posla ne bi mogli u razumnom vremenskom roku izvesti procjenu rizika, odnosno taj postupak kada bi ga radili interni auditori predugo bi trajao.

Nakon procjene rizika, izrađuje se Izvješće o procjeni rizika te se priprema Plan postupanja sa rizicima za one rizike koji se ne mogu prihvatiti. Taj plan može obuhvatiti kontrole kojima će se ti rizici prenjeti na treće strane poput osiguravajućih društava ili podatkovnih centara te kontrole kojima će se rizici izbjegavati. Kontrole za umanjenje rizika mogu se odabrati iz niza preporučenih kontrola Priloga A norme ISO 27001. Ako organizacija uvodi ISMS sustav koji planira i certificirati, nužno je izraditi „Izjavu o primjenjivosti" (*eng. SOA-Statement of Applicability"* u kojoj mora obrazložiti razloge odabira kontrola iz Priloga A. Određene

[69] Krakar Zdravko i suradnici; Korporativna informacijska sigurnost, Fakultet organizacije i informatike Varaždin 2014. Str. 149.

kontrole mogu se odbaciti samo u slučaju da u konkretnoj organizaciji nisu primjenjive. Na temelju Plana postupanja sa rizicima rade se potrebne sigurnosne politike, procedure, radne upute i zapisi, a preporuka je isto primjenjivati u dinamici u kojoj određeni dokument i nastaje. Na kraju svake implementacije ISMS-a nužno je provesti adekvantnu edukaciju djelatnika na svim razinama organizacije i upoznati djelatnike sa onim segmentima ISMS-a koji se odnose na njih te podizati svijest o značaju informacijske sigurnosti i poštivanju pravila definiranih ISMS-om. U DUZS-u edukaciju će provesti interni auditori, dok će za podizanje svijesti o informacijskoj sigurnosti biti zaduženi operativni menadžeri.

Jedna od preporuka za operativne menadžere je upoznati svoje podređene sa „Politikom čistog ekrana i čistog stola“, jer u DUZS, bilo koji sektor ili odjel nerijetko dolaze posjete službenih osoba iz drugih organizacija poput djelatnika Hrvatske vojske, policije, komunalnih poduzeća, predstavnika lokalne i regionalne samouprave, novinari te razne udruge građana, učenici i studenti. Županijski centar 112 svake godine ugošćuje polaznike Ratne škole među kojima ima i vojnih časnika iz vojski drugih zemalja te na“Dan 112“ koji se obilježava 11.veljače svake godine ugošćuje i učenike iz osnovnih škola, naravno uz prethodnu najavu.

Interni auditori obavezno provode procjene ISMS-a, a na osnovi dobivenih rezultata koji se dostavljaju upravi, uprava donosi ocjenu ISMS-a. Ovakav mehanizam osigurava da se uoče postojeći nedostaci u ISMS-u te provode njegova poboljšanja.

Nakon svega, uprava poziva vanjske auditore (pravne osobe koje se bave certifikacijom organizacije), koji obavljaju procjenu ISMS-a te ako je sve u redu, organizacija dobiva cerfikat po normi ISO/IEC 27001.

Jedna od preporuka je da se interne procjene i ocjene sustava od strane uprave provode minimalno jednom godišnje. Ovime će organizacija ostvariti sve prednosti koje su opisane u prethodnom tekstu ovog završnog rada, a na dobiti će biti svi djelatnici organizacije te prepoznati kao ozbiljni partneri u poslovnom svijetu.

5.3. Elaboracija hipoteze

U ovom radu prezentirana je tema informacijska sigurnost u poslovanju. Kroz ovaj završni rad, hipoteza o postojanju norme po kojoj se implementira i certificira sigurnost informacijskog sustava, a time i informacijska sigurnost u poslovanju, potvrđena je. Kao potvrda ove hipoteze u ovom završnom radu obrađene su norme iz serije ISO 27000 koje se odnose na informacijsku sigurnost u poslovanju. Svaka norma sadrži kontrole kojih se svaki djelatnik treba pridržavati, kako bi se osigurala povjerljivost, cjelovitost i integritet informacijskog sustava.
Također ovu normu može implementirati odnosno certificirati se po njoj bilo koja organizacija u svijetu bez obzira čime se bavi. Opisani su koraci u implementaciji norme, što sve učiniti te čega se pridržavati u zaštiti informacijskog sustava a time i osigurati informacijsku sigurnost u poslovanju na korist svih (organizacije,djelatnika, vlasnika, dobavljača, financijskih institucija te države).

6. ZAKLJUČAK ZAVRŠNOG RADA

Jedan od najvažnijih ciljeva svake organizacije je osiguranje neprekinutosti odnosno kontinuiteta poslovanja. U današnje vrijeme kontinuitet poslovanja zavisi od više faktora koji na njega utječu, jedan od tih faktora dakako je informacijska sigurnost tj. zaštita podataka i ostalih resursa u poslovanju.

Informacijska sigurnost je proces, što znači da se neprekidno razvijaju novi sustavi zaštite informacijskog sustava. Razlog tomu je neprekidan razvoj novih alata koji mogu ugroziti sigurnost informacijskog sustava poput „zloćudnog“ *softwarea* (npr.virusi) koji mogu prilikom upada u informacijski sustav napraviti veliku štetu, poput krađe podataka, koji mogu dovesti i do krađe novčanih sredstava sa bankovnih računa. Isto tako razvijaju se i novi načini poslovne špijunaže, koja ne mora biti samo računalne prirode.

Rezultat implementiranja normi informacijske sigurnosti (serije ISO 27000) dobiva se jasno definiran okvir nadležnosti, odgovornosti i ovlasti unutar informacijskog sustava odnosno organizacije. Implementacija navedenih normi prilično je složen postupak koji zahtjeva ulaganje ne samo ljudskog rada i znanja već i financijskih sredstava. Kao glavni dio implementacije normi naveo bih procjenu rizika, koja obuhvaća svaki resurs u poslovanju, od materijalne imovine, financijske imovine do onog najbitnijeg i najvrednijeg u svakoj organizaciji a to su – ljudi odnosno zaposlenici. Što je procjena rizika rigoroznija, to će implementacija normi biti skuplja, a time i informacijska sigurnost bolja.

Uvođenje sustava upravljanja sigurnošću informacijskog sustava te implementacija normi iz serije ISO 27000 predstavlja provedbu potrebnih mjera za postizanje zadovoljavajuće razine informacijske sigurnosti unutar organizacije.

Na taj se način omogućava nesmetanost obavljanja djelatnosti organizacije, a organizacija postaje prepoznata kao pouzdan i moderan poslovni partner, koja se u svakom trenutku može suočiti s najnovijim sigurnosnim prijetnjama i na vrijeme reagirati na eventualne sigurnosne incidente.

LITERATURA

Knjige i priručnici:

1. Krakar Zdravko i suradnici; Korporativna informacijska sigurnost, Fakultet organizacije i informatike Varaždin 2014.
2. Kondić Ž; Kvaliteta i ISO 9000, Tiva Varaždin 2002.
3. Kostanjevec A. i dr.. Sigurnost informacijskih sustava verzija 01012014, FOI Varaždin 2014
4. Lazibat T; Upravljanje kvalitetom; Znanstvena knjiga zagreb, 2009
5. Luić Lj.: Informacijski sustavi, Veleučilište u Karlovcu, 2009
6. National security and the future, Vol.13, No.3., Udruga Sv.Jurja Zagreb, rujan 2012
7. Praktični menadžment; Vol.2. No.2. Prosinac 2011. Visoka škola za menadžment u turizmu i informatici u Virovitici
8. Šehanović J. i dr.: Informatika za ekonomiste, Sveučilište u Rijeci, Pula 2002
9. Uredba o unutarnjem ustrojstvu Ministarstva unutarnjih poslova Republike Hrvatske, (NN 70/2012)
10. Zakon o informacijskoj sigurnosti, NN (79/07)
11. Zbornik radova; Dani kriznog upravljanja 2011. Veleučilište Velika Gorica 2011.
12. Zbornik radova Veleučilišta u Šibeniku, No.1-2/2015, srpanj 2015,

Zakoni i uredbe:

1. Uredba o unutarnjem ustrojstvu Ministarstva unutarnjih poslova Republike Hrvatske, (NN 70/2012)
2. Zakon o informacijskoj sigurnosti, NN (79/07)

Internet izvori:

1. CRN, https://www.crn.com.au/news/10-reasons-why-iso-27001-makes-a-better-is-security-professional-152262 (30.10.2017).
2. Ministarstvo vanjskih i europskih poslova: http://www.mvep.hr/hr/vanjska-politika/multilateralni-odnosi0/medunarodna-sigurnost/racviac/ (31.10.2017).
3. Web stranice kolegija „Sigurnost informacijskih sustava“ pri Fakultetu organizacije i informatike Varaždin. ; http://security.foi.hr/wiki/index.php/Glavna_stranica , (30.10.2017).

POPIS SLIKA

Slike