ФАКУЛТЕТ ЗА ИНДУСТРИЈСКИ МЕНАЏМЕНТ
АСОЦИЈАЦИЈА ЗА КВАЛИТЕТ И СТАНДАРДИЗАЦИЈУ СРБИЈЕ
УНИЈА ПОСЛОДАВАЦА СРБИЈЕ
XIII Научно стручни скуп "Систем квалитета услов за успешно пословање и конкурентност"
Врњачка Бања 24. - 26.11.2011. године, Хотел Бреза

MJERENJE UČINKOVITOSTIINFORMACIJSKE SIGURNOSTI

Zdenko Adelsberger, Krešimir Buntak, Dejan Adelsberger[1]

Rezime: *Implementacije sistema upravljanja informacijskom sigurnošću (ISMS) prema standardu ISO 27001 predstavlja u cjelini vrlo složeni projekt, kao i kasnije nakon certifikacije, upravljanje s njime. Od niza raznih elemenata ISMS koji ga određuju kroz ispunjavanje zahtjeva standarda, područje mjerenja informacijske sigurnosti je jedno od najtežih i najkompleksnijih, jer ima najmanje praktičnog iskustva. Upravo ta težina određivanja mjernih parametara i metodologije mjerenja sigurnosti informacijskog sistema dovodi do toga da se menadžeri i auditori zadovoljavaju elementarnih (formalnim) rješenjima s upitnom stvarnom vrijednošću. U radu se daje prikaz metodologije mjerenja efikasnosti informacijske sigurnosti i ukazuje na ključne probleme implementacije mjerenja.*

Ključne riječi: *informacijska sigurnost, rizici, mjerenje, optimizacija procesa*

1. UVOD

Svi sistemi upravljanja temeljeni na standardima serije ISO imaju između niza zahtjeva koje se mora ispuniti i upravljanje pomoću PDCA (Plan-Do-Check-Act) kruga. Naravno, taj zahtjev je uvjetovan ako se želi dokazati sukladnost sa standardom i na temelju toga dobiti certifikat, kao dokaz te sukladnosti.

Pod PDCA krugom se smatraju četiri faze ciklusa upravljanja bilo kakvim sistemom: faza planiranja (P) u kojoj se detaljno planira što, kako, koliko i sa čime se želi nešto postići, faza napravi(D) u kojoj se realizira ono što se sve planiralo u P fazi, faza provjeri (C) u kojoj se provjerava da li su se postigli svi očekivani rezultati planirani u P fazi, te na kraju faza djeluj (A) u kojoj se u slučaju potrebe zbog odstupanja postignutih rezultata u odnosu na planirane predviđaju korektivne i/ili preventivne radnje, odnosno poboljšanje.

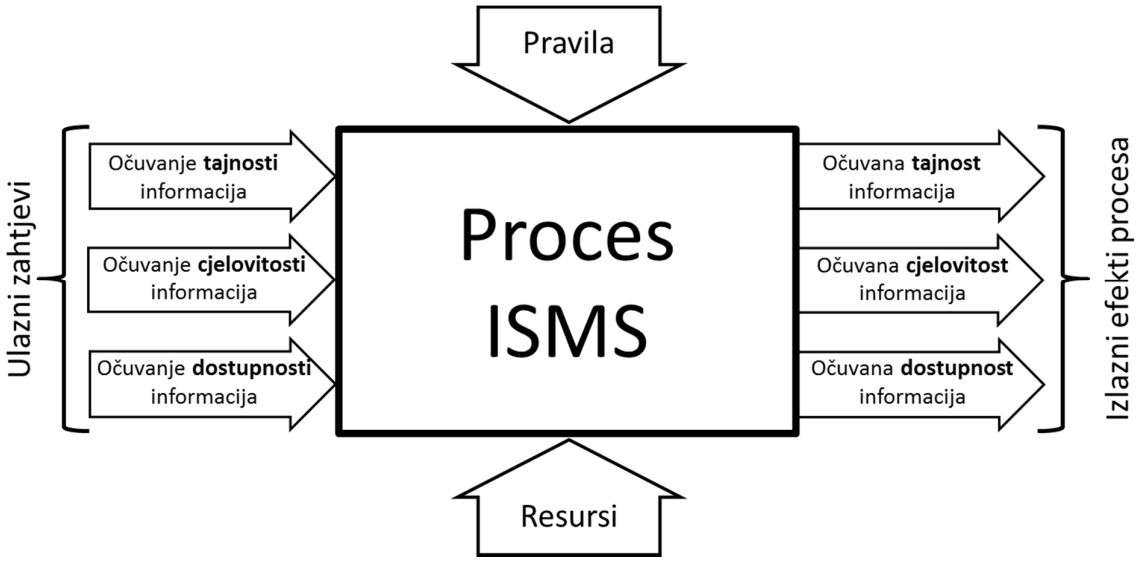
Iz gore navedenog je očito da se postignuti rezultati u C fazi moraju mjeriti da bi se mogli uspoređivati sa planiranim (očekivanim) rezultatima u P fazi. Upravo ta mjerenja su ključ uspješnog funkcioniranja usvakom sistema upravljanja. Naime, ako nisu u dovoljnoj mjeri planirana mjerenja i kontrola očekivanih rezultata, tada se ni od sistema upravljanja ne može očekivati značajna efikasnost i doprinos u povećanju vrijednosti. Ako se ne može dokazati utjecaj nekog sistema upravljanja na povećanje vrijednosti, onda taj sistem upravljanja nitine treba organizaciji.

Upravo iz razloga presudnog značaja mjerenja u okviru sistema upravljanja u okviru ovog rada će se prikazati praktični primjer implementacije mjerenja u okviru sistema upravljanja informacijskom sigurnošću (ISMS), temeljeno na implementaciji standarda ISO 27001:2005. Pored toga, treba naglasiti da je opisani princip u potpunosti primjenljiv na sve sistemeupravljanja(ISO 9001, ISO 14001, OHSAS 18001, itd.).

[1]Mr.sc. Zdenko Adelsberger, Bluefield d.o.o., Zagreb, HR, zadelsbe@zg.t-com.hr
[2] Dr.sc. Krešimir Buntak, DZM RH, Zagreb, RH, kresimir.buntak@dzm.hr
[3] Dejan Adelsberger, Bluefield d.o.o., Zagreb, RH, dejan@bluefield.hr

2. ISMS I ZAHTJEVI ZA MJERENJEM EFIKASNOSTI

U okviru standarda ISO 27001:2005 definira seniz zahtjeva koji se morajuispuniti ako se želi postići certifikat. Pod pojmom ISMS (InformationSecurityManagement System), odnosno sistem za upravljanje informacijskom sigurnošću smatra se proces u kojem se pomoću resursa, pravila i načina ponašanja svih uključenih faktora ulazni zahtjevi pretvaraju u njihovo zadovoljenje na izlazu. Blok shema procesa ISMS prikazana je na slici 1.



Slika 1. Blok shema procesa ISMS prema ISO/IEC 27001:2005

Kao što se može vidjeti sa slike 1., prema ISO/IEC 27001:2005 postoje tri obavezna ulazna zahtjeva koja se funkcioniranjem ISMS procesamoraju zadovoljiti. Ti ulazni zahtjevi su: očuvanje tajnosti, cjelovitosti i dostupnosti informacija. Prema engleskim nazivima za ova tri zahtjeva (**C**onfidentiality i **I**ntegrity i **A**vailability) često se koristi akronim C-I-A. Na temelju angažiranja resursa u skladu s pravilima ISMS procestreba zadovoljiti ova tri zahtjeva.Tako se na izlazu procesa može dogoditi da su ulazni zahtjevi zadovoljeni u cijelosti, djelomično ili nikako, svi ili samo neki od njih. Da bi se moglo reći da ISMS procesdobro funkcionira, odnosno uspješno zadovoljava ulazne zahtjeve morajuse znati kriteriji na temelju kojihse donosi ocjena o stupnju zadovoljenja ulaznih zahtjeva, te način mjerenja tog stupnja zadovoljenja. To se općenito izražava mjerom efikasnosti[2] i učinkovitosti[3]. U praksi to znači provesti niz mjerenja na temelju kojih se može točno utvrditi efikasnost, ali i učinkovitosti uspostavljenog ISMS procesa. U cilju određivanja mjesta u procesu na kojima će se vršiti mjerenja i odrediti kakva mjerenja provesti potrebno je mapirati poslovni ISMS proces. Kako je mapiranje ISMS procesa složena aktivnost u ovom radu se neće posvećivati pažnja tom pitanju, ali korisnicima koji žele implementirati i poboljšavati ISMS na principima efikasnosti i učinkovitosti to je neizbježna potreba.

3. ZAHTJEVI ZA MJERENJIMA U ISO/IEC 27001:2005

U okviru standarda ISO/IEC 27001:2005 nalazi se niz mjesta na kojima se eksplicitno zahtijevaju mjerenja na uspostavljenom ISMS-u. To naravno nisu sve obaveze za mjerenjem. Postoji još niz drugih mjesta u ISMS procesu na kojima treba planirati i provoditi mjerenja, a zavise u prvom redu od ozbiljnosti

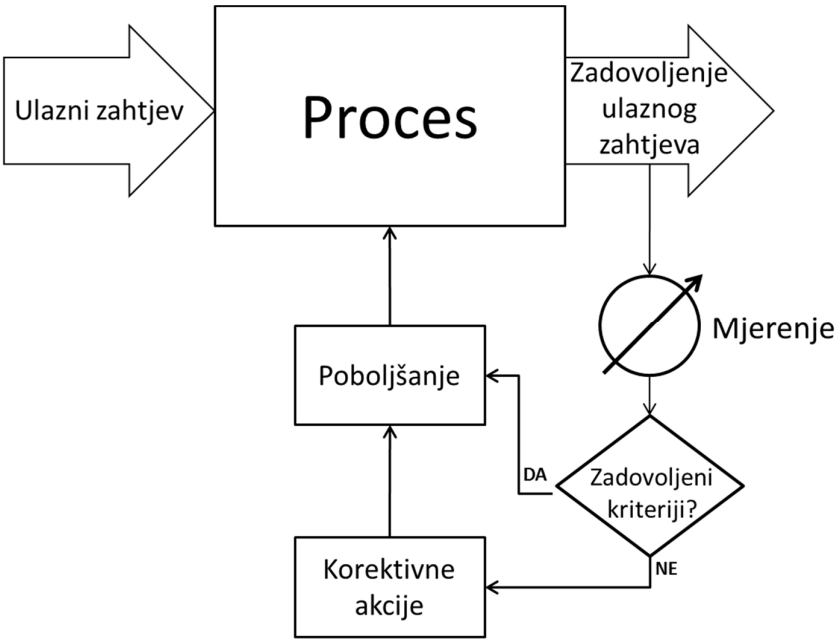
[2] Efikasnost se definira kao ostvarenje nekog cilja s minimumom troškova, napora ili gubitaka.
[3]Učinkovitost (efektivnost) je pojam pod kojim se podrazumijeva izvođenje pravih stvari (aktivnosti) koje dovode do ostvarenja cilja.

uspostavljenog ISMS-a i teġnje za poboljġanjem, ali i svijesti da se sa sistemom moġe dobro upravljati samo ako su i mjerenja uļinkovita.

Pogledajmo sada na kojim mjestima ISO/IEC 27001:2005 eksplicitno zahtjeva mjerenja:

- 0.2 Procesni pristup: é d) kontinuiranog poboljġanja temeljenog na objektivnom mjerenju.
- é Procijeniti i gdje je primjenjivo, mjeriti izvrġavanje procesa u odnosu na ISMS politiku, ciljeve i praktiļno iskustvo te izvjeġtavati upravu o rezultatima radi provjere.
- 4.2.2.d) Odrediti naļin mjerenja uļinkovitosti odabranih kontrola ili grupa kontrola i definirati naļin na koji Íe ta mjerenja biti korigtena u procjeni uļinkovitosti kontrola, tako da rezultiraju usporedivim i ponovljivim rezultatima.
- 4.2.3.b) Izvoditi redovitu provjeru uļinkovitosti ISMS-a (ukljuļujuÍi zadovoljavanje ISMS politike i ciljeva, te provjeru sigurnosnih kontrola) uzimajuÍi u obzir rezultate sigurnosnih audita, incidente, rezultate mjerenja uļinkovitosti, prijedloge i povratne informacije svih zainteresiranih strana.
- 4.2.3.c) Mjeriti uļinkovitost kontrola kako bi se provjerilo da su zadovoljeni sigurnosni zahtjevi.
- 4.3.1.g) Organizaciji potrebne dokumentirane procedure koje osiguravaju uļinkovito planiranje, rad i kontrolu njenih procesa informacijske sigurnosti, te opisuju kako mjeriti uļinkovitost kontrola.
- 7.2.f) Rezultate mjerenja uļinkovitosti
- 7.3.e) Poboljġanja naļina mjerenja uļinkovitosti kontrola

Ovaj kratki pregled mjesta u standardu upuÍuje da se bilo kakvo ocjenjivanje uspostavljenog ISMS-a temelji na mjerenjima, odnosno usporedbi postignutih rezultata mjerenja i planiranih (oļekivanih). Osnovni princip funkcije mjerenja prikazan je na slici 2. Prikazana shema principa mjerenja vrijedi za procese i podprocese do nivoa aktivnosti.



Slika 2. Blok shema principa mjerenja i njegovog utjecaja na proces

Moġe se vidjeti da su mjerenja osnova korektivnih aktivnosti, kao i planiranja poboljġanja. Kriteriji prihvatljivosti mjerenja se definiraju u P fazi implementacije PDCA kruga za proces.

4. MJERENJE UČINKOVITOSTI PROCESA ISMS

Iz prethodno iznesenog evidentno je da se problemu mjerenja uļinkovitosti procesa ISMS mora pristupiti vrlo ozbiljno i promiġljeno jer su mjerenja kao aktivnosti ugraĽene u temelje funkcioniranja procesa.

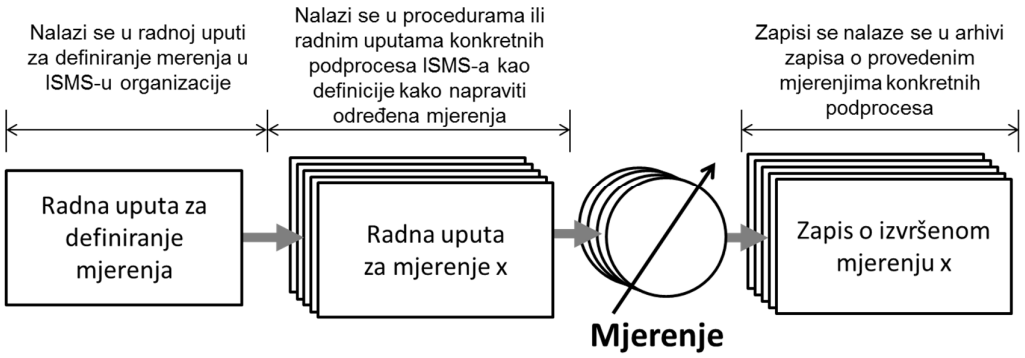
Da bi takva mjerenje imala smisla ona trebaju ukljuļivati slijedeĺe ciljeve:

a) Procjenu uļinkovitosti implementiranog ISMS-a
b) Procjenu uļinkovitosti implementiranih procesa
c) Provjeru ispunjenosti prepoznatih zahtjeva zainteresiranih strana
d) Olakġano poboljġanje ISMS u smislu ukupnih informacijskih rizika;
e) Davanje prijedloga za ocjenu uprave za lakġe odluļivanje vezano za ISMS, donoġenje odluka i opravdavanje zahtjeva za unapreĽivanje implementiranog ISMS

Posebna paġnja se mora posvetiti osnovnim principima na kojima se bazira prihvatljivo mjerenje:

a) Svi rezultati mjerenja moraju biti dokazivi
b) Svi rezultati mjerenja moraju biti ponovljivi
c) Mjerenja moraju nastojati iskljuļivati subjektivnost ï ġto je u nekim sluļajevima vezano za poslovne procese teġko izbjeĺi

Da bi se postigli ti ciljevi kao i u svakom drugom sluļaju kada se radi o implementaciji niza aktivnosti treba definirati proces ili radnu uputu za obavljanje istih. Kada se radi o mjerenju, tada je primjereno za svaku vrstu mjerenja definirati radnu uputu koja Ĺe ukljuļivati i kriterije prihvatljivosti rezultata mjerenja. Blok shema organizacije i provoĽenja takvog mjerenja koje zadovoljava gore spomenute principe prikazana je na slici 3.

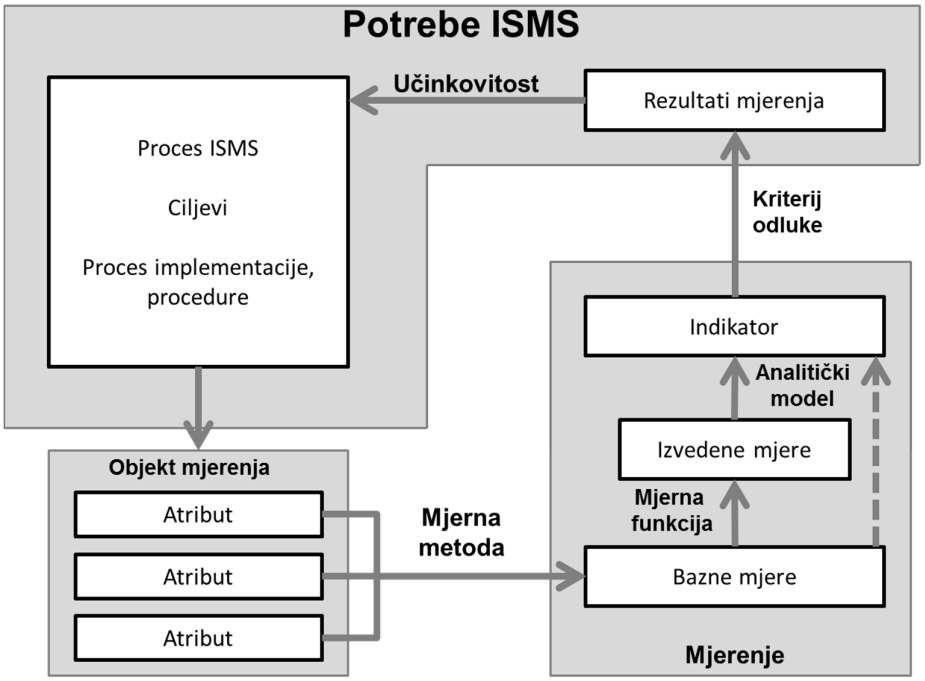


Slika 3. Blok shema organizacije i provođenja mjerenja u sistemu upravljanja

Oļito je da treba prvo definirati radnu uputu pomoĺu koje se generiraju pravila za mjerenje bilo kojeg parametra procesa. Na temelju te radne upute moguĺe je generirati pravila mjerenja i kriterije ocjene mjerenja bilo kojeg parametra procesa na jedinstveni naļin. Da bi se moglo odrediti elementi za radnu uputu potrebno je detaljnije pogledati parametre mjerenja i meĽusobne odnose u korelaciji sa procesom na kojemu se ġeli provesti mjerenje. Na slici 4. je prikazana blok shema mjerenja i vezana proces ISMS, ali i bilo koji drugi proces.

Nakon ġto se odabere neki objekt mjerenja (proces, podproces), na njemu treba prepoznati atribute koji ga definiraju u smislu mjerenja. Prema identificiranim i odabranim atributima objekta koje se ġeli mjeriti potrebno je definirati mjernu metodu. Tih mjernih metoda moġe biti najviġe onoliko koliko ima i odabranih atributa.

Pod mjernom metodom se smatra logički slijed informacija, općenito opisan i korištten u kvantificiranju atributa u skladu sa određenom skalom. Vrsta metode mjerenja ovisi o prirodi operacija korištenih za kvantificiranje atributa. Raspoznaju se dvije vrste: subjektivna (kvantifikacija koja uključuje ljudsku procjenu) ili objektivna (kvantifikacija bazirana na numeričkim pravilima).



Slika 4. Blok shema sistema mjerenja učinkovitosti procesa ISMS-a

Primjenom mjerne metode dobivaju se rezultati u tzv. baznim mjerama. Pod pojmom „mjera" se podrazumijeva veličina (varijabla) koja sadrži vrijednost mjerenja nekog atributa. Izraz „mjerao se koristi za referenciranje za bazne mjere, izvedene mjere i indikatore. U pojedinim slučajevima bazne mjere nisu dovoljne, pa se pomoću mjerne funkcije dobiva tzv. izvedena mjera. Pri tome se pod pojmom „mjerna funkcija" podrazumijeva algoritam ili kalkulacija izvedena kombiniranjem dviju ili više baznih mjera. Slijedom blok sheme na slici 4. se u slijedećem koraku definiranja radne upute za mjerenja primjenjuje se analitički model, koji predstavlja algoritam ili kalkulacije koje kombiniraju jedno i/ili više baznih i/ili izvedenih mjera sa pridruženimkriterijima za odluku. Primjenom analitičkog modela kao rezultat dobivaju se indikatori, odnosno pokazatelji koji su koriste za donošenje odluka na temelju kriterija odluka. Indikator je mjera koja pruža procjenu određenog atributa izvedenog iz analitičkog modela u skladu sa definiranim informacijskim potrebama, a kriterij odluke su pragovi, ciljevi, ili uzorci korišteni za određivanje potrebe za akcijom u daljnjoj istrazi, ili za opis razine pouzdanosti u danom rezultatu. Rezultat mjerenja koji se dobiva primjenom kriterija odluke je jedan ili više indikatora i njima pridružene interpretacije koje se odnose na željenu informaciju. U konačnici na temelju tako definiranog mjerenja i rezultata mjerenja se dobiva informacija o učinkovitosti mjerenog objekta.

Formalno radna uputa za definiciju mjerenja treba da ima slijedeće dijelove:

a) Identifikacija mjerenja(naziv mjerenja, ID mjerenja, opis razloga mjerenja, ciljna kontrola/proces za mjerenje – planirana ili implementirana)
b) Definiranje objekta mjerenja i atributa (objekt mjerenja karakteriziran kroz atribute mjerenja, atributi mjerenja)
c) Definiranje osnovnih specifikacija za mjere - za svaku baznu mjeru (bazna mjerenja, metoda mjerenja, vrste metode mjerenja, mjerna skala, tip skale, jedinica mjerenja)

d) Definiranje specifikacije izvedene mjere (naziv izvedene mjere, mjerna funkcija)
e) Definiranje specifikacije indikatora (indikator, analitički model)
f) Definiranje specifikacije kriterija za odluku
g) Definiranje rezultatamjerenja(interpretacija indikatora, forme izvještavanja)
h) Identifikaciju zainteresiranih strana (korisnici mjerenja, recenzent mjerenja, vlasnik informacije, sakupljač informacija, komunikator informacija)
i) Definiranje Frekvencije/Perioda mjerenja i vađenja pravila mjerenja (frekvencija prikupljanja podataka, frekvencija analize podataka, frekvencija izvještavanja rezultata, revizija mjerenja, period mjerenja).

Forma kako zapisati radnu uputu kao dokument treba biti u skladu s procedurom za upravljanje dokumentacijom kao obaveznom u okviru ISMS.

Neki od procesa i točaka mjerenja učinkovitosti u okviru ISMS-a su: ISMS trening, ISMS-osposobljeno osoblje, Trening informacijske sigurnosti,Trening svjesnosti za ISMS, Politika lozinki,Kvaliteta lozinke - ručno definirano, Kvaliteta lozinke - automatsko definiranje, ISMS proces nadzora, Neprekidno poboljšavanje informacijske sigurnosti za upravljanje incidentima, Implementacija korektivnih aktivnosti, Predanost uprave, Zaštita od zlonamjernog koda, Kontrole fizičkog pristupa, Pregled log datoteka, Upravljanje periodičkim održavanjem, Sigurnost u ugovorima sa trećim stranama, itd.

5. ZAKLJUČAK

Na temelju iznesenog može se vidjeti da je pristup problemu mjerenja učinkovitosti ISMS (ali i bilo kojeg drugog sistema upravljanja) te poslovnih procesa vrlo ozbiljan i složen zadatak. Ozbiljnost i složenost definiranja načina mjerenja i interpretacije rezultata mjerenja direktno je vezana za stav vrhovne uprave o ozbiljnosti uspostavljanja ISMS-au organizaciji. Što je veća težnja vrhovne uprave za ozbiljnom uspostavom i poboljšanjem ISMS-au organizaciji to se zahtjeva više raznih mjerenja učinkovitosti i ozbiljniji pristup definiranju svakog pojedinom mjerenja.

LITERATURA

1. ISO/IEC 27001:2005, Informationtechnology – Securitytechniques – information security management systems – Requirements
2. ISO/IEC 27004:2009, Information technology – Security techniques – Information security management – Measurement
3. Jaquith Andrew, *Security Metrics: Replacing Fear, Uncertainty, And Doubt*, Addison-Wesley Professional, 2007
4. Kovacich Gerald L., Halibozek Edward, *Security Metrics Management: How To Manage The Costs Of An Assets Protection Program*, Butterworth-Heinemann, 2005
5. Peltier Thomas R., *Information Security Policies And Procedures: Guidelines For Effective Information Security Management*, Auerbach PublishersInc., 2008
6. Bao Jie, Lee Peter L., *Process Control: The Passive Systems Approach (Advances I nIndustrial Control)*, Springer, 2007