E-MAINTENANCE MANAGEMENT IN E-BUSINESS PROCESSES OF DIGITAL COMPANIES

Ramona Markoska[1], Aleksandar Markoski[2], Mitko Kostov[3], Mile Petkovski[4]

Tehnički Fakultet - Bitola, Republic of Macedonia
[1]ramona.markoska@tfb.uklo.edu.mk, [2]aleksandar.markoski@tfb.uklo.edu.mk,
[3]mitko.kostov@uklo.edu.mk, [4]mile.petkovski@uklo.edu.mk.

Abstract: The process of maintaining ICT infrastructure in digital companies is very important for the quality and safety of e-business processes. E-maintenance as a synonym for the maintenance of ICT infrastructure includes a wide range of activities that must be considered from several aspects.This paper provides an overview of each item, which is an important part of e - maintenance: lifetime use of ICT solutions, the process of replacement of ICT equipment, identification and implementation of new ICT trends, adjustment of existing and new ICT components, and safety aspects.
These recommendations are the dynamics of change and the development of e-business processes to digital companies. The importance of the recommendations are more at the level of the universal rules of conduct and operating procedures that are not strictly related to existing solutions. E - business processes, in general, with the initial information that is transforming the way it creates a new value of the information. Furthermore, the quality, reliability and protection of information is a key task in the e - maintenance. Therefore, e-maintenance, is aimed at the prevention of safety and quality assurance of information related to e-business processes. In this context, the approach given in this work is based on the concept of existing international standards of information security.

Keywords: E-maintenance, ICT infrastructure, e-business

MENADŽMENT E-ODRZAVANJA U E-BIZNIS PROCESIMA DIGITALNIH KOMPANIJA

Ramona Markoska, Aleksandar Markoski, Mitko Kostov, Mile Petkovski

Abstract: Menadžment odrzavanja IKT infrastrukture u biznis procesima digitalnih kompanija, je veoma važan za kvalitet i sigurnost e-biznis procesa. E-održavanje kao sinonim održavanja IKT infrastukture, obuhvata široki spektar aktivnosti, koje moraju biti menadžirani sa vise aspekata. U ovom radu je dat pregled svih značajnih kompomenti e-održavanja: vek trajanja i zastarivanja korišćenih IKT rešenja, procesi zamene IKT opreme, prepoznavanje novih trendova, usaglašavanje postojećih i novih komponenti, sigurnosni aspekti. Pritom se polazi od dinamike promena i razvoj samih e- biznis procesa u digitalnim kompanijama. Date preporuke su vise na nivou univerzalnih smernica i radnih procedura koje nisu striktno vezane za postojeća rešenja. E-biznis procesi, generalno, uzimaju informaciju kako sirovinu i transformišu je na način da joj dodaju vrednost. Stoga, kvalitet, pouzdanost i zaštita informacije je ključni zadatak i procesima e-održavanja. Samim tim menadžment održavanja IKT infrastrukture, u velikoj meri je

nasočen ka prevenciji obezbeđivanja i kvaliteta samih informacija, relevantnih u e-biznis procesima.U tom kontekstu, korišćen je pristup koji uzima u obzir postojeće svetske sigurnosne standarde informacione sigurnosti.

Ključne reči: E-održavanje, ICT infrastruktura, e-biznis

1.UVOD - PROBLEMI E-ODRŽAVANJA

Sam proces održavanja u jednoj kompaniji može se razmatrati na dve razine: opšte preporuke i univerzalna načela, kao i specijalna organizacija koja uzima u obzir sve taskove i specifičnosti koje proizlaze od načina rada i samog procesa stvaranja vrednosti i proizvodnje u kompaniji. Proces proizvodnje kod digitalnih kompanija, je organizovan na način da su u velikoj meri prisutni digitalizovani procesi. Ali isto tako, postoje i klasčni procesi, koji su unapređeni korišćenjem IKT rešenja. To znači da savremeni menadžment održavanja poseduje e-održavanje kao jednu novu komponentu, koja je prilagođena specifičnostima novih IKT solucija. Dalje, sa druge strane treba imati u vidu, da se u prilagođenom procesu proizvodnje u kontekstu stvaranja nove vrednosti, prvi put pojavljuje i sama informacija i njena obrada, pa je samim tim e- održavanje, prilagođeno i samoj informaciji. U tom kontekstu, e-održavanje se svodi na oblasti IKT infrastrukture, što podrazumeva tretman hardverskih i softverskih solucija, kao i brigu o kvalitetu, pouzdanosti i sigurnosti informacije[1],[2]. Glavna dopunska karakteristika e-održavanja je mogućnost predikcije i prevencije svih pretnji koje se odnose na pouzdanost rada IKT sistema i bezbednost samih informacija, tokom njihovog transfera unutar digitalne kompanije, kao i u komunikaciji za svim saradnicima i klijentima. Imajući u vidu postojane promene, napredak i uvođenje novih tehnologija, e-održavanje je veoma dinamična oblast koja uporedo mora pratiti i sve pretnje koje dolaze od web orientiranog načina rada u samim digitalnim kompanijama.

2. ELEMENTI E-ODRŽAVANJA

Glavni cilj e-održavanja se sastoji u obezbeđivanju neprečenog rada svih ICT solucija u digitalnoj kompaniji, što podrazumeva i zaštitu relevantnih informacija u različitim fazama njihove obrade. Polazeći od karakteristike samih e-biznis solucija kao i online načina rada, iskustvo je pokazalo da je najbolji način e-održavanja, u suštini predikcija i prevencija u najvećoj mogućoj meri.

Menadžment e-održavanja se svodi na sledeće radne stavke [5] :

A. *Organizacija radnih procesa na način koji omogućuje maksimalnu zaštitu samih IKT solucija i informacija* koje su u isto vreme i radni resurs, polufabrikat a često i finalni i glavni produkt. Što se tiče same organizacije radnih procesa, postoje radne procedure i preporuke za menadžment bezbednosne IKT infrastrukture, kao i standardi informacione sigurnosti koji obezbeđuju minimizaciju verovatnoće bilo kakvog incidenta.
B. *Analiza svih mogućih incidenata koji se mogu pojaviti u napomenutim oblastima*, što se u praksi svodi na menadžment komponenti i infrastrukture primenjenih IKT

solucija, obezbeđivanje fizičke sigurnosti, kao i sigurnosni tretman informacijskog toka.

C. *Prevencija svih inicidenata*, u kontekstu da budu sprečeni gde god je to moguće, korišćenjem saznanja i primenom preporuka koje se temelje na prethodne stavke, A i B.
D. *Sanacija svih incidenata* koji ne mogu da budu sprečeni, u kontekstu izradnje propisanih radnih procedura za njihovo što brže otklanjanje. Ovo je veoma inventivna faza, koja polazi od toga da se nikad ne može izbeći neki incident sa stoprocentnom sigurnošću, ali se zato dobrom organizacijom može minimizirati vreme disfunkcionalnosti, kako i obim potencijalne štete.

Što se tiče same organizacije radnih procesa, postoje radne procedure i preporuke za menadžment bezbenosne IKT infrastrukture, kao i standardi informacione sigurnosti koji obezbeđuju minimizaciju verovatnoće bilo kakvog incidenta.

3. MENADŽMENT E-ODRŽAVANJA U DIGITALNIM KOMPANIJAMA

Treba napomenuti da su prethodno navedeni elementi e-održavanja, razdvojeni sa ciljem uspostavljanja distinkcije od klasičnog održavanja u kompanijama. Sa aspekta potrebnih aktivnosti menadžment e-održavanja uglavnom se svodi na menadžment IKT infrastrukture, i menadžment informacione sigurnosti. Zahtevi održavanja uglavnom se svode na obezbeđivanje neprečenog kontinuiranog rada, sa minimalnim zastojima zbog realizacije samih taskova održavanja[3]. Dalje, ciljevi savremenog menadžmenta e-održavanja mogu se klasificirati u sledeće kategorije:

- Iznalaženje formaliziranih pristupa za upravljanje rizikom, Root Cause analiza
- Primena savremenih strategija održavanja, kao što sum Reliability Centred Maintenance , RCM, što je održavanje zasnovano na doverljivosti, i Total Productive Maintenance, TPM, t.j. poptuno produktivno održavanje.
- Integracija uticaja ljudskog faktora
- Primena participativnog pristupa u projektovanju i odabiru opreme i hardvera, Designfor Maintainability, Value Engineering, Hazop.

3.1. INFORMACIONI SYSTEM U FUNKCIJI E-ODRŽAVANJA, COMPUTERISED MAINTENANCE MANAGEMENT SYSTEM

Iako ne spada u klasične strategije e-održavanja, korišćenje informacionih sistema je trend koji je u podemu kao savremena alatka za analizu postojećeg sistema održavanja [4]. Analiza se sastoji u sledeće dve faze:

- *Procena sistema*, koja se temelji na odgovore na sledeće stavke:
    1. Kako deluju preventivne procedure na broj korektivnih aktivnosti
    2. Dali je preventivno održavanje redovno i dali su rezultati zadovoljavajući, imajući u vidu da je sistem dobar ukoliko je na 6 preventivnih aktivnosti prisutna jedna korektivna.
    3. Lociranje kritičnih mesta sa aspekta doverljivosti, u pogledu hardvera, softvera, lokacije
    4. Vreme potrebno za izvršavanje pojedinih aktivnosti

5. Broj aktivnih taskova održavanja u proseku
6. Troškovi održavanja

- *Identifikacija problema*, koja se zasniva na sledećim analizama:

1. Usklađenost softvera
2. Pregled i popis opreme- vid, tip, lokacija, doverljivost, pripadnost celini, zastarivanje, rok trajanja, kompatibilnost
3. Rezervni delovi i urgentna rešenja
4. Analiza povratne veze efikasnosti preventivnih mera

Analize nedvojbeno pokazuju da je korišćenje IKT opreme instalirane za poddršku samih e-biznis procesa za uspostavljanje jednog informacionog sistema u funkciji e-održavanja, investicija koja se isplati za 18 do 30 meseci.

3.2. STRATEGIJE E-ODRŽAVANJA U E-BIZNIS PROCESIMA

Imajući u vidu dinamiku promena i specifičnosti koje sa sobom nose razna IKT rešenja koja se primenjuju i kombiniraju za raznim sistemima za podršku u odlučivanju kao i sa biznis inteligencijom, oblasti od značaja za e-održavanje se mogu klasificirati na sledeći način:

- *Korektivno održavanje*, koje se svodi na planiranje, predikciju i saniranje nastalih objektivnih poremećaja i diskunkcionalnosti.
- *Preventivno održavanje*, koje ima za cilj obezbeđivanje dobre kondicije održavanja, što podrazumeva menadžment svih potencijalnih problema pre njihovog nastajanja. Ovaj način održavanja ima za cilj minimizaciju svih mogućih disfunkcionalnosti.
- *Inspektivno održavanje*, se na neki način povezuje sa preventivnim održavanjem i predstavlja njegov operativni deo. Statistika mogućih incidenata, njihova lokacija, analiza kritičnih radnih uslova su osnova za planiranje inspektivnog održavanja.

Treba napomenuti da su sve tri nabrojene strategije univerzalne i primenjivane i pre nastanka samog e-biznisa.

3.2.1. Incidentan menadžment e-održavanja

Kao specifična kategorija menadžmenta održavanja, incidentni menadžment je zadužen za problem korektivnog održavanja. Polazna tačka planiranja raznih aktivnosti je fakt da je rok trajanja IKT rešenja ograničen sa aspekta zastarivanja, kompatibilnosti I doverljivosti pri radu. To se odnosi na sav hardver ali i na softverska rešenja koja mogu raditi sa unapred proračunatom sigurnošću i očekivanom greškom. Korektivni menadžment se bazira na konceptu da se unapred predvide svi mogući problemi kao i način njihove sanacije, imajući u vidu da je vreme njihovog nastanka stohastično [1]. Cilj incidentnog menadžmenta u e-održavanju je lokalizacija i minimizacija vremena disfunkcionalnosti e-biznis sistema. Incidentni menadžment se uglavnom svodi na dve važne aktivnosti:

- *Prioritet incidenata*, koji se brine o definisanju i uspostavljanju tačno određenog prioriteta rešavanja problema ukoliko se pojave vise njih u istom trenutku, imajući u vidu njihovu međusobnu povezanost.

- *Vremensko optimiranje*, koje podrazumeva pronalaženje strategija i planiranje samog procesa rešavanja nastalih incidenata sa ciljem da se optimira vreme sanacije nekog incidenta.

3.2.2. Rizik menadžment u e-održavanju, kako kompilacija preventivnog i inspektivnog menadžmenta

Ova specifična komponenta menadžmenta e-održavanja pretstavlja kombinaciju raznih radnih procedura *inspektivnog* i *preventivnog* menadžmenta. Analizom samih biznis procesa na nivou komponenti i aktivnosti može se unapred sa određenom verojatnošću presmetati kakve su šanse za defekte i smetnje u radu [6]. Samim tim što se sa smanjenjem rizika, u isto vreme povećava sigurnost i pouzdanost u radu, kako sinonim sreće se i naziv *sigurnosni menadžment*. Postoje određene dopirne tačke ali i jasna distikcija između inspektivnog i preventivnog menadžmenta:

- *Inspektivni menadžment* kao deo sigurnosnog menadžmenta, zadužen je za dinamiku izvođenja kontrola i inspekcija sa ciljem da se obezbede adekvatni podatci. Planovi i strategije se zasnivaju na nekoliko različitih kategorija podataka:
  a. Podatci proizvoditelja hardvera i softverskih rešenja o pouzdanosti i načinu rada
  b. Sopstvena radna iskustva kompanije
  c. Iskustva drugih korisnika i suradnika

- *Preventivni menadžment*, kao deo sigurnosnog menadžmenta bavi se sa promocijom raznih planova i procedura sa ciljem da se preduhitre kad god je to izvodljivo, sve eventualne havarije, zastoji u radu i eventualne greške. Kako bazične aktivnosti u tom smeri se preporučuju:
  a. *Preventivna zaštita hardvdera* koja podrazumeva aktivnosti zamena zastarene opreme, pre nego se dese havarije. Ove aktivnosti polaze od toga dali je ekonomičnije da se određeni stari delovi IKT solucija zamene iako su ispravni, uporedbom troškova zamene sa troškovima nastale štete u slučaju havarije. U ovom drugom slučaju na cenu zamene delova ili softvera, dodaju se i poslovne zagube u period zastoja radi havarije.
  b. *Zaštita od neovlašćenog pristupa i izrada sigurnosnih strategija,* koja se odnosi na rad softverskih solucija. Interesantno je da sami sigurnosni upadi mogu biti sprečeni sa raznim zaštitnim tehnikama i procedurama koje se odnose i na hardverska konfiguraciona rešenja, zajedno sa softverskim zaštitama. Jedno od mogućih rešenja je uspostavljanje sigurnosne arhitekture mrežne opreme [5].

3.3. NIVOI IMPLEMENTACIJE MENADŽMENTA E-ODRŽAVANJA ZA IKT SOLUCIJE

Preznetirane činjenice navode na to da se menadžment e-održavanja može razmatrati na različnim nivoima:

- *Nivo mrežne arhitekture*, koje obuhvata sve aktivnosti odabira i usklađivanja IKT opreme, koje se dalje može razmatrati kao:
  a. Menadžment održavanja mrežnih hardverskih komponenata
  b. Menadžment održavanja mrežnih usluga i servisa

- *Softversko nivo*, koje se brine o interoperabilnosti i stabilnosti svih korišćenih softverskih solucija, koje se odnose na interpersonalnu komunikaciju unutar kompanije, dalje, sa klijentima i suradnicima. Takođe, obuhvata i sva bezbednosna rešenja i standarde za zaštitu od virusa i drugih sigurnosnih upada.

- *Nivo elektronskih komunikacija*, koje tretira sve segmente telekomunikacijskih usluga, relevantne za neprečeno finkcioniranje e-biznis procesa. U ovom domenu spadaju postupci sigurnosnog prenosa informacija, alternativno preusmeravanje elektronskog saobraćaja, realne potrebe neprekidne telekomunikacijske veze, u korelaciji sa nivoima tolerancije na prekide, sagledani isključivo sa metapozicije konkretnog e-biznis procesa.

Sva navedena nivoa su data kao kategorije vise opisno nego suštinski, sa cilljem distinkcije raznih radnih specifičnosti. [3],[4]. Tako, treba imati u vidu da je IKT solucija za e-biznis, praktično, sva oprema, t.e. sav hardver i softver podređen radu u mreži, kao u kompaniji, tako i globalno, u međusobnoj povezanosti posredstvom elektronskih komunikacija.

3.4. MENADŽMENT INFORMACIONE SIGURNOSTI I PRINCIP NAJMANJE PRIVILEGIJE

Korišćenje interneta u e-biznis procesima, za potrebe elektronske interkomunikacije, čak i u slučajima menadžiranog i personalizovanog saobraćaja, donosi sa sobom uvećane rizike koje se odnose na sam proces transfera informacija kao i na njihove pouzdanosti i bezbednosti. Kao rezultat raznih istraživanja i sistematizacije radnih iskustava kompanija i raznih institucija, uspostavljena je serija sigunosnih standarda, koje propisuju način organizacije i rada sa informacijama, sa ciljem obezbeđivanja informacione sigurnosti. Treba napomenuti da ovi standardi prate aktuelni momentat na svetskom nivou što se tiče informacione sigurnosti, te stoga permanentno evoluiraju. Na početku je uspostavljen Britanski standard BS 7799, koji je osnova za kasnije verzije BS 7799 part 1 ISO/IEC 17799, koji je kasnije modificiran i unapređen u BS 7799-2, iz koga proizlazi, ISO/IEC 27000, i njegove varijante iz 2005 I 2013 godine [8].

Napomenuti informacioni standardi, ukratko, što se tiče informacione sigurnosti, nalažu kao osnovne sledeće tri komponente:

- *Doverljivost*, što podrazumeva obavezu da se obezbedi autorizovani pristup do svake informacije, i tačno nivo privilegija nad njom.
- *Integritet*, što podrazumeva obezbeđivanje i garanciju tačnosti, potpunosti i celovitosti samih informacija i metoda za njihove obrade.
- *Dostupnost*, podrazumeva obezbeđivanje adekvatnih prava i privilegija, raznim grupama autorizovanih korisnika.

Obezbeđivanjem adekvatne doverljivosti, integriteta i dostupnosti, postiže se *Princip najmanje privilegije*, koji se odnosi na multy-user informacione sisteme. Po ovom principu, svakom korisniku treba da budi dodeljeni ona prava i privilegije koja su potrebna i dovoljna za izvršenje njegovih aktivnosti. Svaka informacija i aktivnost, koja nije neophodna, ukoliko je dopuštena, pretstavlja potencijalnu pretnju po bezbednost. Razumljivo, potrebno je postojanje t.n, *privilegovanog pristupa*, poznatog kako *root*

access, kakav imaju administratori sistema koji su zaduženi za menadžment e-održavanja, putem obezbeđivanja komponente informacione sigurnosti.

Kao rezultat svih ovih aktivnosti koje nalažu nabrojane komponente, postiže se nivo informacione sigurnosti koje obezbeđuje zaštitu informacija a samim tim, kontinuitet i pouzdanost e-biznis procesa, sa aspekta informacione sigurnosti.

4. SOFTVERSKI BAZIRANI E-MENADŽMENT

Pored sigurnosne arhitekture postoje i softverska rešenja sa strogo određenom namenom, da menadžiraju određene softverske probleme. Ove aplikacije su koncipirane na principima samoanalize, samodetekcije i samoreparacije, a koriste se za specifičnu problematiku softverskog održavanja kao deo e-održavanja u e-biznis procesima.

Pritom, one menadžiraju razne softverske probleme:

- *Menadžment konfiguracionih problema*- Može se desiti tokom rada da odjednom bez ikakvog razumljivog razloga, određeni delovi (softver, hardver) prestanu sa pouzdanim radom. Isto tako, moguće su situacije da se određene aktivnosti koje se bez ikakvih problema izvršavaju na drugim kompjuterima u mreži, na nekoj radnoj stanici ne mogu izvršiti. Ovakvi se problemi rešavaju snimanjem zapisa registra, svih radnih stanja, sva podešavanja hardvera i softvera sa ciljem njihovog upoređivanja, da bi se locirao i sanirao neki problem. Treba napomenuti da se ovo odnosi na probleme sa softverom, ali i hardverom, kad su u pitanju drajveri ili procedure konfiguracije.
- *Reparativni ili Patch menadžment*, se odnosi na sve situacije kad su potrebna određena premoščivanja, zakrpe, popravke, reparacije nekog promenjenog radnog stanja. Uglavnom se na ovaj način saniraju bezbednosni propusti povezani sa online radom. Softver namenjen za ovaj cilj mora biti interakvitan i prediktivan.
- *Spyware menadžment*, se odnosi na posebnu grupu problema, kada su informacije bez znanja korisnika ili kompanije, prikupljene sa ciljem ostvaruvanja neke nelegalne koristi ili nanošenje štete. Softver namenjen za ovaj cilj mora biti fokusiran na određene ciljne informacije i njihove maksimalne zaštite. Uglavnom, to su osetljive informacije lične prirode, ili velikog biznis značaja.

4.1. SAMOREPARATIVNI I SAMOKONFIGURACIONI MENADŽMENT

Menadžment e-održavanja sledi trendove u domenu IKT solucija koje se koriste u e-biznis procesima, prilagođavajući se permanentno novitetima. Da bi ti napori bili uspešni, nekad je neophodno predivdeti u kom pravcu treba očekivati promene. Velike softverske korporacije imaju studije koje proučavaju uticaj ovih očekivanih promena na strategisku formulaciju i implementaciju menadžmenta e-održavanja.

U tom pravcu, očekuju se sledeći trendovi:

- *Samoreparativni i samokonfiguracioni menadžment*, koji se odnosi na softverske probleme, t.j. rad aplikacija i konfiguriranje hardvera, po analogiju reparacije u živim organizmima posredstvom genetskih algoritama[7]. Ovo je veoma aktuelan i savremen pristup.
- *Prioritet prediktivnom menadžmentu*, što podrazumeva analizu sa ciljem predikcije mogućih upada, sa ciljem njihove prevencije umesto sanacije.
- *Menadžment uvođenja novih tehnologija*, sa ciljem njihovog permanentnog usaglašavanja sa postojećim koje se već primenjuju, čime se postiže evolucija e-biznis sistema umesto, revolucionarne promene koje bi tražile veće investicije i prekide u radu.

5. ZAKLJUČAK

Procesi e-biznis transformacije uvode velike promene u način poslovanja, samim tim što je obrada i tok informacije jedan sasvim novi dopunski segment o kome se mora voditi račun. Uvođenje novih tehnologija, koje se neprestano izmenjuju, sam fakt da postojeće IKT solucije zastarevaju u relativno kratkom periodu od nekoliko godina, kao i njihov način ukpapanja i kombiniranja sa postojećim klasičnim rešenjima, nalažu više dimenzija menadžmenta održavanja. Jedna od tih dimenzija je proučavanje klasičnih strategija i metoda menadžmenta održavanja, i njihovo prilagođivanje e-biznis situaciji. Ponekad, to nije dovoljno, pa je potrebno kreirati sasvim nove strategije. Menadžment e-održavanja, je zato, dinamičan i interaktivan kako i sama srž e-biznis procesa. E-održavanje počinje tako što sledi trendove menadžmenta održavanja kako početno stanje i radni okvir, ali njegova suština je praćenje modaliteta rada e-tehnologije koja omogućuje e-biznis procese. Veoma aktuelan segment je tretman samih informacija, posebno u domenu zaštite ličnih podataka i poslovno relevantnih informacija, što sa sobom vuče i neke dopunske implikacije. Menadžment e-održavanja se stoga, može i treba posmatrati kao aktivnost za čije je uspešno sprovođenje potrebna moderirana strategija koja obedinjuje pravila klasičnog menadžmenta održavanja i određene strategije socijalne komunikacije, u koju su potrebni skilovi predikcije i prevencije na bazi procene. Sa jedne strane je klasična biznis okolina koja je osavremena sa IKT solucijama, sa druge strane su standardi informacione sigurnosti i procedure koje su se koristile za obezbeđivanje sigurnosti informacija u raznim razuznavačkim agencijama. Ta dva, navidum, nespojiva stajališta, u kombinaciji sa postojanim napretkom IKT solucija i socijalnim implikacijama e-biznisa, daju menadžmentu e-održavanja jednu dimenziju kontrolirane stohastičnosti, što ga čini veoma zanimljivim za istraživanje i unapređivanje.

REFERENCE

1. Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., and Zajicek, M. (2004). “Defining incident management processes for csirts: A work in progress” (No. CMU/SEI-2004-TR-015). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

2. Bhaskar, R. (2005). “A Proposed Integrated Framework for Coordinating Computer Security Incident Response Team”. *Journal of Information Privacy & Security*, *1*(3)
3. Braithwaite, T. (2002) “Securing E-Business Systems: A Guide for Managers and Executive”
4. Ladan, M. I. (2013). “E-business Security Chalenges”. *The Second International Conference on Digital Enterprise and Information Systems (DEIS2013)* (pp. 159-165). The Society of Digital Information and Wireless Communication.
5. Markoska,R., Jolesvski, I. (2009) “Perimetar sigurnosti i menadžment bezbednosne IKT infrastructure u e-biznis procesima”, E-Trgovina, Palić
6. Sukumar, A., Edgar, D., & Grant, K. (2011). “An investigation of e-business risks in UK SMEs” . *World Review of Entrepreneurship, Management and Sustainable Development*, *7*(4), 380-401.
7. Wang, Y. M. (2007). “Computer Genomics: Towards Self-Change and Configuration Management” *Microsoft Research*.
8. ISO 27001 Central http://www.17799central.com/