

BEZBEDNOSNA SVEST, OBUKA I EDUKACIJA – KRITIČNE KOMPONENTE ZAŠTITE KIBER-PROSTORA

prof. dr Slobodan R. Petrović,
Udruženje sudskih veštaka za informacione tehnologije

Apstrakt: *U radu se ukazuje na drastične i dramatične promene koje u ljudskom društvu izaziva eksplozivno širenje informacione tehnologije, praćene rizicima sa potencijalno nesagledivim posledicama i na potrebu, prava i odgovornost društvene zajednice da se adekvatno zaštiti. S tim u vezi posebno se akcentiraju bezbednosna svest, obuka i edukacija svih učesnika informacionih procesa, kao kritične komponente zaštite kiber-prostora.*

Ključne reči: *kiber-prostor, zaštita, bezbednosna svest, obuka i edukacija.*

SECURITY AWARENESS, TRAINING AND EDUCATION – CRITICAL COMPONENTS OF CYBER-SPACE SECURITY

Professor Slobodan R. Petrović, Ph.D.
Association of Information Technology Experts

Abstract: *This paper is dealing with critical and dramatic changes caused by explosive dissemination of information technology in the society, along with risks from potentially unforeseeable consequences and the need, right and responsibility of the community to protect itself against them. Also, security awareness, training and education of all participants in the information process as a critical component of cyber-space security are emphasized.*

Key words: *cyber-space, security, security awareness, training, education.*

*"Metode koje će najefektnije minimizirati mogućnost napadača da kompromituju informacionu zaštitu su opsežno i sveobuhvato obučeni i edukovani korisnici. Propisivanje politika i procedura jednostavno neće zadovoljiti. Čak i njihovo nadgledanje može biti neefikasno: moj pristup do Motorole, Nokie, ATTa, Suna zavisio je od spremnosti ljudi da zaobilaze politike i procedure koje su bile uspostavljene godinama pre nego što sam ih ja uspešno kompromitovao."*¹

Kevin Mitnick

1. UVOD

Jedna od ključnih odrednica vremena u kojem živimo svakako je buran razvoj informacione tehnologije i njena sve šira primena u svim sferama ljudske delatnosti, od trivijalnih do složenijih i krajnje komplikovanih. Vidljivo je i golim okom da eksplozivni razvoj i eksponencijalni rast primene informacione tehnologije kreiraju novu elektronsku opciju koja sve šire i dublje prekriva društvenu zajednicu, menjajući i drastično i dramatično globalni ambijent čovekovog življenja, stvarajući neophodne pretpostavke da se sve radi brže, lakše, obimnije, kvalitetnije i jeftinije.²

U tom novom ambijentu informaciona tehnologija postaje glavni, a sve češće i jedini alat za obavljanje sve brojnijih i raznovrsnijih aktivnosti i poslova, a kiber-prostor u sve većoj meri postaje opšte mesto događanja za sve poznate ljudske aktivnosti: od informisanja, komuniciranja, edukacije i zabave, preko kooperacije u realnom vremenu, obavljanja i izvršavanja raznih poslovnih, administrativnih i drugih aktivnosti i obaveza, kontrole i upravljanja složenim aktivnostima i procesima, pa do najsloženijih oblika kriminalne delatnosti, špijunaže i terorizma. Iako se još uvek nalazimo na samom početku nove (informacione) ere, ova tehnologija sa promenama koje izaziva uveliko nagoveštava pretvaranje digitalnog univerzuma u vitalni resurs koji suočava pojedince, grupe i nacije sa izazovima adaptiranja, inoviranja i reagovanja na mnoge do skora nezamislive prilike i mogućnosti koje im se ukazuju.

Dakle, informaciona tehnologija menja svet u meri da ništa više nije i neće biti kao ranije. Te promene, usmerene prvenstveno na način na koji živimo, učimo, radimo i komuniciramo, odvijaju se u najvećoj meri na revolucionaran način, zbog čega su i označene nazivima koji u sebi sadrže pomenutu odrednicu – *Računarska revolucija, Komunikaciona revolucija, Informaciona revolucija, Internet revolucija, Multimedijalna revolucija, ...*

Ključni simboli ovih promena, koje su *brze, duboke, široke i raznovrsne* u meri da ih je često teško *shvatiti, prihvatiti i pratiti*, označeni terminološkim nazivima – računari, računarski programi, programski jezici, računarske mreže, serveri, klijenti. ... – veoma jasno najavljuju jedno novo doba, doba koje takođe ima razne nazive – *Digitalno doba, Binarno doba, Informaciono doba, Informaciono društvo, ...* Međutim, nezavisno od naziva, te promene se dešavaju u svim slojevima društva i u svim delovima sveta, a njihove konsekvence će se značajno prelamati kroz ceo naš životni vek. Jednostavno, možda prejako, ali sigurno adekvatno rečeno, informaciona tehnologija postaje vitalna sve više u onoj meri u kojoj je vitalan i vazduh koji udišemo.

2. EFEKTI I IMPLIKACIJE

Sviđalo se to nekom ili ne, činjenica je da ekspanzija informacione tehnologije i automatizacija poslovnih aktivnosti i procesa u svim sferama društvenog života zaista

¹ Security Awareness Toolbox, IWS – The Information Warfare Site,
<http://www.iwar.org.uk/comsec/resources/sa-tools>

² Petrović R. S., Kompjuterski kriminal, Vojnoizdavački zavod, Beograd 2004.

predstavljaju istinski fenomen današnjice – fenomen koji polako, ali sigurno, kreira društvo ekstremno zavisno od znanja, a ta zavisnost će se vremenom samo širiti i pojačavati. Zbog mogućih negativnih implikacija koje proizilaze iz činjenice da ova tehnologija sve više preuzima i najvitalnije funkcije ljudske delatnosti, da pruža sve više i sve raznovrsnije servise svojim korisnicima i da se sve više vrednih duštvenih dobara pretvara u bitove i smešta u računarske sisteme, zbog čega društvena zajednica postaje osetljivija, odnosno ranjivija i izloženija brojnim rizicima, postoji neminovna potreba da se promene, koje su u toku i koje će tek nastati pod delovanjem informacione tehnologije, što bolje sagledaju i razumeju u meri koja će omogućiti i olakšati naše individualno i kolektivno prilagođavanje novim uslovima i na taj način stvoriti pretpostavke da se u najvećoj meri i na najbolji mogući način iskoriste sve prednosti, pogodnosti i mogućnosti koje informaciona tehnologija tako nesebično pruža, a da se istovremeno spreči njena zloupotreba.³

Zaključak koji se nameće svakako je da pomenuta potreba nije ni laka ni jednostavna. Posebno što je transformacija u informaciono društvo krcata ne samo poželjnim pogodnostima, već i vrlo ozbiljnim rizicima, čije potencijalne implikacije i konsekvence nije lako ni sagledati ni predvideti. Upravo zato, proces transformacije ne bi smeo da se odvija potpuno spontano, već je neophodno na njega, u granicama raspoloživih mogućnosti, uticati, kontrolisati ga i usmeravati njegove tokove. Ovo utoliko pre jer su rapidni rast i globalizacija računarskih mreža, sa konglomeratom ljudi, računara, veza, sadržaja i mogućnosti, široko otvorili vrata i brojnim zloupotrebama informacione tehnologije koje su bez presedana.

Brojni rizici, kao što su narušavanje poverljivosti i privatnosti, remećenje vitalnih operacija, destrukcija intelektualnih dobara, razne vrste prevara i krađa i mnogo drugog, i to na način i u obimu o čemu se pre samo nekoliko decenija nije moglo ni sanjati, ukazuju da se suočavamo sa izazovima koji se, najjednostavnije rečeno, moraju držati pod kontrolom. U protivnom, ovo može da preraste u vrlo ozbiljne probleme sa posledicama od kojih mnoge nije lako ni predvideti, a njihove dimenzije ni naslutiti. Sve ovo ima još veću težinu ako se zna da smo na ivici eksplozije u obimu elektronskih podataka i informacija koji se u digitalnoj formi razmenjuju na pojedinačnoj i grupnoj osnovi preko globalne informacione infrastrukture. Predstavljajući *kiber-dobra* različitog nivoa vrednosti i značajnosti, kao što su informacije različitog stepena značajnosti i tajnosti, razna vrsta robe, intelektualna dobra i novac, ove digitalne forme iskrsavaju kao najvrednija valuta Informacionog doba. Sadržaji koji se kreiraju u računarima, skladište na diskovima i prenose preko komunikacionih linija postaju vredniji od računara, diskova i mrežnih elemenata preko kojih se prenose. Zbog svega toga društvena zajednica ima *potrebu, prava, obavezu i odgovornost* da štiti svoje ogromno bogatstvo smešteno u virtuelnom kiber-prostoru.

Međutim, imajući u vidu ozbiljnost, obimnost i složenost zaštite nacionalnog informacionog ambijenta, koja je po značaju adekvatna zaštiti nacionalnog vazdušnog prostora, ovako jasnu konstataciju je daleko lakše izreći nego praktično realizovati. Razlog tome su svakako, s jedne strane, dimenzije i složenost problema koji treba rešavati, a sa druge strane naša poslovična nepripremljenost i neobučenost u meri koja bi nam mogla garantovati određeni uspeh.

³ Mittal N., Nault R. B., Investments in Information Technology: Indirect Effects and Information Technology Intensity, Haskayne School of Business University of Calgary, Canada, February 4, 2005, http://www.haskayne.ucalgary.ca/research/WorkingPapers/research/media/MIS_working_papers/2005-16.pdf; Seifert W. J., Petersen R. E., House of Representatives Information Technology Management Issues: An Overview of the Effects on Institutional Operations, the Legislative Process, and Future Planning, Report for Congress, Updated July 25, 2002.

3. ZAŠTITA KIBER-PROSTORA

GAO (General Accounting Office) je još 1997. godine identifikovao informacionu zaštitu kao novu visoko-rizičnu zonu koja praktično dotiče sve važnije aspekte funkcionisanja društva.⁴ Identifikovani su ključni faktori od kojih su neki ne tehnološki, već ljudski faktori, kao na primer, nedovoljna svest i nerazumevanje rizika informacione zaštite kod učesnika u informacionim procesima, oskudno dizajnirani i implementirani programi zaštite, deficit kadrova sa tehničkim iskustvom potrebnim za upravljanje kontrolama i limitirana kontrola pravila tehničke eksploatacije. Sve ovo dokazuje i ranije uočenu činjenicu da su ljudi, koji su i inače po svojoj prirodi skloni greškama, prepoznati kao najslabija karika u sistemu zaštite.

Ono što je proizašlo iz spomenute identifikacije jeste da su ključ za označavanje ljudskih faktora ili kompetencija *svest, obuka i edukacija*. Pri tome, cilj bezbednosne svesti, obuke i edukacije jeste da se ojača zaštita i to:

- poboljšavanjem svesti o potrebi zaštite informacionih resursa;
- razvijanjem i usavršavanjem veština i znanja da korisnici mogu bezbednije izvršavati svoje poslove;
- produbljivanje znanja, kada je potrebno, za dizajniranje, implementaciju ili operisanje programa zaštite.

Izvesno je da potreba za širom pažnjom prema ovoj oblasti IT zaštite nikada nije bila veća, zbog čega je ova potreba posebno aktuelna. Jer, upravo zbog tog ljudskog faktora smo puno vremena izgubili i puno mogućnosti propustili da već zakoračimo duboko u informaciono društvo i da u velikoj meri koristimo njegove blagodeti. Zaštita je oduvek bila ozbiljan i obiman problem, kojem se najčešće nije posvećivala zaslužena pažnja. To i takvo stanje su koristili protivnici informatizacije, štiteći svoje ranije stečene pozicije ozbiljno ugrožene novom tehnologijom, da spreče promene pravdajući to mogućim negativnim konsekvencama. Njihov broj, kao i njihov uticaj ni danas nije zanemarljiv. Jednostavno nisu spremni da se upuštaju u neizvestan rizik i to u oblasti u kojoj nisu dorasli, pre svega stručno, da, kao što su navikli, vode glavnu reč.

Očigledno je da niko sam ne može zaštititi integritet, poverljivost i raspoloživost informacionih resursa u današnjem ambijentu visoko umreženih sistema, a da ne obezbedi da svaka uključena osoba razume svoju ulogu i odgovornost i da je adekvatno obučena da ih izvršava. Ljudski faktor je u toj meri kritičan za uspeh da američki zakon o zaštiti računara iz 1987. godine (Computer Security Act) zahteva:⁵ *"Svaka agencija će obezbediti obaveznu periodičnu obuku za razvoj svesti o kompjuterskoj zaštiti i prihvatljive kompjuterske prakse svih zaposlenih koji su uključeni u upravljanje, korišćenje ili operisanje bilo kog federalnog kompjuterskog sistema unutar ili pod nadzormo te agencije"*.

Zašto nepoverovati razvijenoj i iskusnoj Americi da je svakom potrebna bazična obuka o konceptima i procedurama zaštite kiber-prostora? Pri tome, mora se znati da problem informacione zaštite nije lokalni problem koji se tako (lokalno) može i rešavati, već on ima nacionalni, a u mnogim segmentima i globalni karakter, zbog čega zahteva učešće svih. Zato je jedan od nacionalnih prioriteta izrada nacionalne strategije zaštite informacionog prostora u kojoj bi se prioriteto fokusirale kritične komponente zaštite informacionog prostora, bez kojih je iluzorno čak i razmišljati o zaštiti: *bezbednosna svesta, obuka i edukacija*. Čak i laicima je postalo jasno da snažan program zaštite informacionog ambijenta zaista ne može biti uspostavljen bez prisustva značajnog

⁴ Information Technology Security Training Requirements: A Role- and Performance-Based Model, NIST Special Publication 800-16, April 1998; Wilson M., Hash J.: Building an Information Technology Security Awareness and Training Program, NIST Special Publication 800-50, October 2003.

⁵ Information Technology Security Training Requirements, op. cit.; Wilson M., Hash J., op. cit.

nivoa *pojedinačne i kolektivne svesti o potrebi zaštite i bezbednosne kulture* svih učesnika, bez snažnog, celovitog i sveobuhvatnog *programa obuke i, najzad, bez kvalitetnog programa edukacije*.

3.1. Bezbednosna svest

Prvi i najznačajniji korak rešavanja problema zaštite kiber-prostora, čiji značaj nije moguće rečima dovoljno naglasiti, jeste donošenje i usvajanje programa izgradnje i razvoja bezbednosne svesti o potrebama, mogućnostima i značaju informacione zaštite. Ovaj program bi trebalo da prekrije celu naciju, sve pojedince koji na bilo koji način učestvuju ili će učestvovati u informacionim procesima, počev od dece predškolskog uzrasta, pa do penzionera najstarijeg životnog doba. Jer, kao što decu odmalena učimo da ne uzimaju samoinicijativno slatkiše u samoposlugama i kako da čuvaju svoje igračke, tako ih moramo naučiti kako da se ponašaju kada se nađu u kiber-prostoru, elektronskim globalnom selu prepunom najraznovrsnijih izazova.

Cilj programa izgradnje bezbednosne svesti je da omogući sagledavanje pretnji i osetljivosti informacionog ambijenta i potencijalnih negativnih posledica, da obezbedi opšte razumevanje problema zaštite informacija i da poboljša ukupnu svest o potrebi i obavezi zaštite informacionog prostora. Fundamentalno poboljšanje svesti o potrebi i prioritetu zaštite informacionog prostora su potrebni da bi se obezbedio snažan podsticaj za izradu i dalji razvoj programa obuke i edukacije iz oblasti informacione zaštite.⁶

Svest je esencijalni element ciklusa upravljanja rizikom i zaštitom i zahteva pažnju na svim nivoima. Bezbednosna svest treba otud da bude usmerena na rukovodioce, korisnike i praktičare informacionih sistema. Svest i razumevanje su esencijalni da bi se implementirala politika informacione zaštite i da bi se obezbedilo da povezane kontrole obavljaju svoje funkcije na odgovarajući i željen način. Ne može se očekivati da će se rukovodioci, korisnici i drugi sa pristupom informacionim resursima složiti sa politikama kojih nisu svesni ili ih ne razumeju. Slično, ako oni nisu svesni rizika povezanih sa njihovim informacionim resursima oni neće moći da razumeju potrebu za podrškom politikama dizajniranim za redukovanje rizika.

Bezbednosna svest upravo podrazumeva shvatanje i razumevanje rizika. Značajan izazov upravljanja rizikom je činjenica da se bezbednosni rizici u informacionom ambijent menjaju vrlo brzo zato što nove osetljivosti i napadački alati kontinualno bivaju identifikovani. Kao konsekvencija ove činjenice statičan proces procene rizika nije više dovoljan. Proces upravljanja rizikom mora sada biti dizajniran da reaguje brzo i stoga treba uključiti elemente procene i odgovora u realnom vremenu.

Elementarne osnove informaciono-bezbednosne pismenosti (bezbednosni termini, koncepti, osetljivosti, pretnje, posledice) se stiču kroz podizanje svesti o potrebi zaštite, a nadogradnja se realizuje kroz obuku, tako da se tranzicija od svesti ka obuci odvija osmišljeno na planiran i očekivan način. Realizacija programa izgradnje bezbednosne svesti o potrebi zaštite informacionog ambijenta na znatno viši nivo od trenutnog je osnovni preduslov za obuku iz zaštite kiber-prostora.⁷

Svest nije obuka. Svrha svesti prezentira se jednostavno sa fokusiranjem pažnje na zaštitu. Prezentacije svesti su namenjene da omoguće pojedincima da prepoznaju i razumeju potencijalne rizike i shodno tome i važnost zaštite.

Efektivna prezentacija bezbednosne svesti mora biti dizajnirana sa ciljem da ljude navede i podstakne na prilagođavanje. Ako se podsticaj koristi u više navrata –

⁶ Information Security: Raising Awareness, Version 1.0, 14 April, 2000, Treasury Board of Canada Secretariat, <http://www.cio-dpi.gc.ca/> ; Information Technology Security Training Requirements, op. cit.

⁷ Information Technology Security Training Requirements ... , op. cit.; Wilson M., Hash J., op. cit.; Information Security: Raising Awareness, op. cit.

ponovljeno, učenik će selektivno ignorisati podsticaje. Dakle, prezentacija svesti mora biti kreativna i podsticajna, sa ciljem da fokusira pažnju učenika tako da će učenje biti inkorporirano u svesno donošenje odluka. Ovo je poznato kao asimilacija kojom pojedinac ugrađuje nova iskustva u svoj postojeći šablon ponašanja.

Svest, kako je originalno definisana u NIST 500-172 "kreira osetljivost [zaposlenih] na pretnje i ranjivost računarskih sistema i spoznaju da treba štititi podatke, informacije i načine njihove obrade. Fundamentalna vrednost programa za bezbednosnu svest je da oni (programi) setuju platformu za obuku donošenjem promena koje menjaju kulturu organizacije. Kulturna promena je shvatanje i razumevanje da je informaciona zaštita kritična zato što bezbednosne greške imaju potencijalno negativne konsekvence za svakoga. *Dakle, informaciona zaštita je posao svih.*⁸

Aktivnosti izgradnje svesti su na nivou informisanja sa ciljem uočavanja, prepoznavanja i pamćenja, a odvijaju se kroz raznorodne aktivnosti/materijale o izgradnji i podizanju svesti o potrebi i mogućnostima informacione zaštite, koji uključuju:

- Popularna prezentaciona predavanja o odabranim temama;
- Diskusione forume o odabranim pitanjima;
- Podsticajno-promotivne poruke sa motivacionim sloganima;
- Bezbednosno-informativni podsetnici (baneri) na računarskom ekranu, koji se pojavljuje kada se korisnik loguje;
- Video trake o bezbednosnoj svesti;
- Bilteni i poster.

3.2 Obuka

Ukoliko se želi ostvariti kvalitetan sistem zaštite značajnu pažnju svakako treba posvetiti obuci korisnika iz domena politike, procedura i tehnika zaštite, kao i upravljačkih, operativnih i tehničkih kontrola potrebnih i raspoloživih za zaštitu informacionih resursa. Kao preduslov i prelaznu aktivnost za obuku iz informacione zaštite pristup bi trebalo da podrazumeva program podizanja bezbednosne svesti na najviši mogući nivo.

"Obuka" kao nivo kontinuuma učenja teži da proizvede relevantne i potrebne bezbednosne veštine i kompetencije praktičara – funkcionalnih specijalista različitih od onih za zaštitu (na primer, rukovodioci, sistem dizajeri, nabavljači, nadzornici i sl.).

Aktivnosti obuke odvijaju se na nivou razumevanja u cilju sticanja osnovnih znanja i veština iz oblasti zaštite, a realizuju se kroz praktičnu instruktazu: lekcije i/ili demonstracije, izučavanje slučajeva, praksa. Ova osnova je nezavisna od specifičnosti informacionih sistema.

Učenje dostignuto kroz jednu jedinu aktivnost o svesti teži da bude kratkoročno, neposredno i specifično. Obuka traje duže i uključuje koncepte i veštine višeg nivoa.

3.3. Edukacija

Edukacija je jasno identifikovana kao separatan nivo učenja namenjen profesionalcima i specijalistima za zaštitu. Obezbeđivanje formalne edukacije i specifičnih kriterijuma edukacionog nivoa za ovu grupu je u nadležnosti programa koje bi trebalo da realizuju akademske ustanove. Smatra se da su edukacija, koja se razlikuje od obuke, i iskustvo povezano sa poslom esencijalni za profesionalce i

⁸ Information Technology Security Training Requirements ... , op. cit.; Wilson M., Hash J., op. cit..

specijaliste informacione zaštite da bi bili u stanju da odigraju svoje uloge na efikasan način.⁹

Aktivnosti edukacije se odvijaju na nivou pronicanja u suštinu problema zaštite u cilju saznavanja, a odvijaju se kroz teoretsku instruktazu (seminari i diskusije, izučavanje i istraživanje). Edukacioni nivo integriše sve bezbednosne veštine i kompetencije različitih funkcionalnih specijalista u jednu zajedničku masu znanja, dodajući multi-disciplinarnu studiju koncepata, pitanja i principa (tehnoloških i socijalnih) i nastoji da proizvede profesionalce i specijaliste zaštite sposobne za predviđanja i pro-aktivne odgovore.¹⁰

4. ZAKLJUČAK

Iz relativno kratkog prikaza kritičnih komponenti zaštite kiber-prostora veoma jasno proizilaze smernice donosiocima odluka na svim nivoima odakle treba početi i u kom pravcu treba usmeravati aktivnosti zaštite kiber-prostora. Konstatacija posebno važi za donosiocima odluka na nacionalnom nivou na kojem se prelamaju, sažimaju i sučeljavaju sve najkrupnije i najvažnije dileme vezane za zaštitu našeg informacionog prostora, a za čiju su bezbednost oni i najodgovorniji. Ovo utoliko pre jer smo našim uključivanjem na Internet ceo naš informacioni prostor izložili na milost i nemilost pojedincima i grupama koji će iz ogromne mase korisnika Interneta, čija je cifra krajem prošle godine premašila milijardu, i sa nečasnim namerama dolaziti u naš informacioni prostor. Pred ovom činjenicom niko nema prava i nesme da zatvara oči. Posebno oni koji imaju i mogućnost i obavezu da reaguju.

5. LITERATURA

1. A Users' Guide: How to Raise Information Security Awareness, June 2006, <http://www.iwar.org.uk/comsec/resources/ENISA/infosec-awareness.pdf>
2. Information Security: Raising Awareness, Version 1.0, 14 April, 2000, Treasury Board of Canada Secretariat, <http://www.cio-dpi.gc.ca/>
3. Information Technology Security Training Requirements: A Role- and Performance-Based Model, NIST Special Publication 800-16, April 1998
4. Operation controls, IT Security Handbook, Version 2.0, November 2001
5. Petrović R. S., KOMPJUTERSKI KRIMINAL, Vojnoizdavački zavod, Beograd 2004, III izdanje, 510 st.
6. Security Awareness Toolbox, IWS – The Information Warfare Site, <http://www.iwar.org.uk/comsec/resources/sa-tools>
7. Wilson M., Hash J.: Building an Information Technology Security Awareness and Training Program, NIST Special Publication 800-50, October 2003
8. Mittal N., Nault R. B., Investments in Information Technology: Indirect Effects and Information Technology Intensity, Haskayne School of Business University of Calgary, Canada, February 4,

⁹ Information Technology Security Training Requirements ... , op. cit.; Wilson M., Hash J., op. cit.

¹⁰ Information Technology Security Training Requirements ... , op. cit.; Wilson M., Hash J., op. cit.

2005,http://www.haskayne.ucalgary.ca/research/WorkingPapers/research/media/MIS_working_papers/2005-16.pdf

9. Seifert W. J., Petersen R. E., House of Representatives Information Technology Management Issues: An Overview of the Effects on Institutional Operations, the Legislative Process, and Future Planning, Report for Congress, Updated July 25, 2002.
10. Shen Z., Yoo Y., Kalle Lyytinen K., Temporal Implications of Information Technology for Work Practices: Organizing in and for Time in an Emergency Department, Proceedings of the 39th Hawaii International Conference on System Sciences – 2006.
11. Significance of Information Technology, *Science & Engineering Indicators* –2002.