UDK: 007:004.056

Prof. dr Boško Rodić,dipl. inž.
mr Milica Tepšić - načelnik Odjeljenja,

KONTROLA U FUNKCIJI PREVENCIJE U INFORMACIONOJ BEZBJEDNOSTI U SISTEMIMA C4I

Rezime

Informacije, pored materije i energije, čine bit vaseljene. Predmet sistema C4I su informacije. Problem je da se (te) informacije zaštite, jer one se (ne)namjerno mogu mijenjati, otuđivati, uništavati, zloupotrebljavati... Za zaštitu informacija razvijaju se sistemi informacione bezbjednosti. Jedan od koraka, posljednji, u razvoju sistema informacione bezbjednosti jeste provjera (kontrola) sistema i, po potrebi, korekcija. Sistem informacione bezbjednosti čine skupovi preventivnih i sanacionih (represivnih) mjera. U ovom radu ćemo dati prikaz primjera kontrole – provjere, kao jedne od (najvažnijih) preventivnih mjera u sistemu informacione bezbjednosti. U literaturi se mogu naći tekstovi u vezi s kontrolom informacione bezbjednosti uglavnom kao preporuke – stavovi.

Ključne riječi: Informacija, komandno-informacioni sistem, informaciona bezbjednost, kontrola.

1. UVOD

Svako vrijeme ima svoje breme koje ga identifikuje, karakteriše i čini drugačijim od ostalih. Kraj XX i početak XXI vijeka obilježila je eksplozija novih tehnologija koje su u potpunosti preoblikovale lice i naličje Planete, uvodeći „ostatak čovječanstva" u Novo doba, koje apologeta Nikolas Negroponte naziva informatičkim dobom. Taj splet nula i jedinica zauvijek je promijenio odnose između centra i periferije, nagovještavajući „vladavinu brojeva", kako to ironično zapaža Pol Virilio, bez koje će život savremenog čovjeka u bliskoj budućnosti biti nemoguć i nezamisliv.

U starom vijeku, u doba Arhimeda[1], trebalo je imati dovoljno jak oslonac i polugu da bi se Zemlja pokrenula. A danas, u djeliću sekunda, Planetu „pokreću" – informacije.

Dakle, kraj prošlog i početak Novog vijeka obilježen je događajima koji sa aspekta razvoja ljudskog roda imaju karakteristike katastrofa (I i II svjetski rat, npr.), velikih istraživačkih poduhvata (lansiranje satelita, odlazak na Mjesec, kloniranje živih bića itd.), ali i kao vijek u kome su izvršene brojne promjene. Navedene promjene se mogu obuhvatiti zajedničkim imenom poznatim kao „talas promjena", ali i kao „megatrendovi". Prema *Johnu Naisbittu* (autor knjige "Megatrendovi"), postoji deset megatrendova, a sa aspekta ovog rada izdvaja se – prelaz iz industrijskog u informatičko društvo[2].

Svjedoci smo burnog vremena u kojem se širom ljudske

[1] Arhimed (grčki: Αρχιμηδης) (287. p. n. e. - 212. p. n. e.), *„Noli turbarecirculos meos*!" – ''Ne dirajte moje krugove!'', bile su posljednje Arhimedove riječi. Smrt ga je zadesila u vrtu, dok je iznad krugova nacrtanih u pijesku rješavao neki geometrijski problem. Ubio ga je vojnik rimskih legija, poslije pada Arhimedove rodne Sirakuze na Siciliji. (Op. M.T.)

2 Prof. dr Boško Rodić, *Poslovni informacioni sistemi*, Fakultet za poslovnu informatiku, Beograd, 2003.

zajednice odvijaju planetarne promjene, prouzrokovane informacionim tehnologijama. Brzina i obim promjena do kojih dovodi korišćenje novih tehnologija, predstavljaju tehnološki presedan, nezapamćen u istoriji ljudske civilizacije. Poznavaoci istorijskih tokova, danas znaju da se u istoriji razvoja ljudskog roda, ništa nije razvijalo tako brzo i imalo veći uticaj na sve promjene u ljudskom društvu od informacione revolucije.

Na žalost, tako velike promjene nose sa sobom i rizik neželjenih posljedica koje, neizbježno, proizlaze iz ovakvih burnih procesa. Zbog toga, posebno zabrinjava činjenica da one mogu postati dominantne u odnosu na željeno stanje. Dakle, veliki izazovi zahtijevaju adekvatne odgovore. Tako bi odgovor na pitanje da li će čovjek u bliskoj budućnosti moći kontrolisati umom ono što je napravio rukom(?) – informacione tehnologije, odredio konture događaja u kojima će biti sasvim jasno da li je čovjek „od svog sluge napravio gospodara"?

2. INFORMACIONA BEZBJEDNOST

Informaciona bezbjednost je nov, složen i u svojoj suštini, višeslojan pojam. Ona je predmet interdisciplinarnih tehničko-tehnoloških (informatika, elektromagnetika, uopšteno obrada signala) i humanitarnih (sociologija, psihologija, pravo, politologija) naučnih istraživanja i kao takva se može posmatrati sa različitih aspekata.

Istorijski posmatrano, informaciona bezbjednost je definisana kao: zaštita informacionih sistema protiv neautorizovanog pristupa ili modifikacija informacija bilo u skladištenju, obradi ili prenosu i protiv lišavanja usluga autorizovanih korisnika, uključujući neophodne mjere detekcije, dokumentovanja i otklanjanja takvih prijetnji.

Bez obzira u kom obliku se čuvaju, prenose i koriste, informacije moraju da budu adekvatno zaštićene. Da bi se osigurala adekvatna zaštita informacija, svi korisnici moraju biti upoznati sa konceptom i mjerama zaštite koje se zahtijevaju. Zaštita informacija, očuvanje njihove povjerljivosti, integriteta, odnosno cjelovitosti i

raspoloživosti, postaje od primarne važnosti. Bezbjednost informacionog sistema štiti informacije od širokog spektra prijetnji u cilju osiguranja kontinuiteta poslovanja, te minimiziranja poslovnih šteta, a maksimiziranja poslovnog uspjeha.

Dakle, informaciona bezbjednost se bavi zaštitom informacija bez obzira u kom obliku one postojale, digitalnom ili papirnom, a informacije se štite ne samo od neovlaštenog pristupa, nego i od uništenja, kao i od neovlaštene promjene.

Potreba za bezbjednošću jedan je od osnovnih motiva djelatnosti ljudi i društva. U praktičnom životu bezbjednost se manifestuje: kao garantovana (konstitucionalnim, zakonodavnim i praktičnim mjerama) zaštićenost životno važnih interesa ličnosti, društva i države; kao nauka, iskustvo i kultura; kao životno važni interesi (ekonomska samostalnost, pravno i socijalno blagostanje, integritet i stabilno i efikasno funkcionisanje); kao svakodnevni, težak, rutinski, ali krajnje važan posao.

Najnoviji filozofski stavovi dijele svemir na tri elementa: materiju, energiju i informaciju. Međutim, Vinerovo (*Norbert Wiener*[3]) određenje informacije da je "... informacija uticaj bilo kog sistema S_1 na sistem S_2", upućuje nas na zaključak da je informacija integrisana i u materiju i u energiju. Naime, spoznaja o prisustvu energije i materije jeste, u stvari, informacija. Informacija je, prema tome, životno važan resurs.

Komandno-informacioni sistemi (KIS): D3 (*Detect, Decide, Destroy*), АСУВ[4] (*Автоматизированная система управления войсками – силами флота*), C2I (*Command Control Intelligence*), C3I (*Command, Control, Communication, Intelligence*), C4I2 (*Command, Control, Communication, Computer, Intelligence and Information*), itd., nisu ništa drugo nego informacioni sistemi sa najvišim mogućim stepenom automatizacije i najvećim mogućim zahtjevima u odnosu

[3] (*November 26, 1894, Columbia, Missouri – March 18, 1964, Stockholm, Sweden*)

[4] Neodvojivi sastavni dijelovi KIS-ova (АСУВ) su, takođe, automatizovani telekomunikacioni sistemi (u originalu – *автоматизированная система связи* – АСС), zatim automatizovani sistemi za upravljanje oružjem (u originalu – *автоматизированная система управления боевыми средствами – АСУБС*) i automatizovani sistemi za upravljanje vatrom (u originalu – *автоматизированные системы управления огнем*). Svi ti elementi u funkcionalnoj vezi čine KIS – АСУВ.

na kvalitet[5] informacije. Prema tome, problemi informacione bezbjednosti u KIS-ovima mogu biti samo rigidniji.

U temeljima američke (SAD) nacionalne bezbjednosti su četiri „kamena temeljca": ekonomska, vojna, diplomatska i **informaciona** bezbjednost. A, informaciona bezbjednost je involvirana u prethodne tri. Nema ekonomske, vojne niti diplomatske bezbjednosti bez informacione.

Sistem informacione bezbjednosti (SIB) ima, u krajnjem, za cilj obezbjeđenje informacione superiornosti C4I sistema

Sistem (informacione) bezbjednosti gradi se načelno kroz pet koraka:

1. Demarkacija potencijalnih (uzročnika) štetnih događaja po informacionu bezbednost.
2. Procjena vjerovatnoće nastupa nekog od štetnih događaja iz tačke 1.
3. Izbor adekvatnih mjera zaštite koje će imati za cilj da preveniraju nastup štetnih događaja iz tačke 1. i da se istim obezbijedi sanacija štete nastale u informacionoj bezbjednosti.
4. Implementacija mjera iz tačke 3.
5. **Provjera** i korekcija mjera iz tačke 4.

Sve mjere, a posebno mjera iz tačke 5, imaju za cilj da preveniraju štetu, posebno da spriječe ili otežaju eventualno namjerno činjenje štete, ili barem da se smanji stepen eventualnih štetnih posljedica.

[5] Pri tome se misli na: blagovremenost, tačnost, potpunost, jednostavnost, po potrebi (najčešće) tajnost, itd.

3. KONTROLA INFORMACIONE BEZBJEDNOSTI U INFORMACIONOM SISTEMU

Kontrola (lat. „*contra*" – suprotan, „*rotulare*" – okretanje) predstavlja posebnu aktivnost permanentnog nadzora vršenja određenih poslova u cilju ostvarivanja zadatih rezultata.

Otvaraju se, najmanje, dva pitanja: šta kontrolisati i kako kontrolisati?

3.1. Šta kontrolisati

Ovo pitanje podrazumijeva (pod)sisteme koji čine informacioni sistem u kom se kontroliše sistem informacione bezbjednosti. Identifikacija podsistema mora biti potpuna i konzistentna. U suprotnom, kao u primjeru najslabije karike, ostaje prostor – slaba tačka u sistemu – za provalu u sistem.

Jedan od pokušaja davanja odgovora na ovo pitanje jeste istraživanje koje je pokrenula Akademija za diplomatiju i bezbednost u Beogradu, zajedno sa Republičkim zavodom za statistiku Republike Srbije.

U momentu pisanja ovog rada objavljeni su rezultati istraživanja.[6] Istraživanje je vršeno na osnovu ankete na uzorku stratifikovanom po veličini i djelatnosti, telefonom. Obim uzorka iznosio je 1.152 preduzeća.

[6] Na primjer [RZS02], na pitanje (u kontekstu kontrole): „Da li vaše preduzeće ima pravilnik kojim su normativno regulisana pitanja informacione bezbednosti?", odgovori su bili očekujući. U bankama i osiguravajućim društvima 77,4% anketiranih odgovorilo je da ima pravilnik. Najlošija situacija je očekujuća – u građevinarstvu. Po pitanju provjere zaposlenih u poznavanju mjera informacione bezbjednosti, opet na prvom mjestu su banke i osiguravajuća društva sa 64,5%, itd.

Slika 1. Elementi informacionog sistema

Moguće polazište koje se sreće u literaturi, u podjeli informacionog sistema na podsisteme koji bi se kontrolisali bilo bi, prema Slici 1, na: *hardware*, *software*, *lifeware*, *orgware, netware* i *dataware*.

Takođe, prema literaturi, [Hsi82], [Int04], [ERY02], [FBI01], [IBM85], [Kpm02], [Muf79], a naročito [How97], moguće je identifikovati podsisteme – elemente sistema informacione bezbjednosti.

Moguća sistematizacija faktora informacione bezbjednosti data je i kao, prema (*IMPLEMENTATION GIDELINES, Appendix A – Minimum Security Requirements for NIPRNet-Internet Connectivity*):

- administrativna (upravna) bezbjednost – podrazumijeva organiza-cione mjere radi bezbjednosti,
- bezbjednost informacionog sistema – podrazumijeva bezbjednost informacija pri obradi, skladištenju i prenosu, podrazumijevajući pristup preko NIPRNet-internet konekcije,
- bezbjednost osoblja – kojom se determiniše ponašanje osoblja,
- fizička bezbjednost – mogućnost planiranja *backup* procedura u slučaju prekida rada servisa i zaštita opreme radi sprečavanja neautorizovanog uvida u informacije, uništavanja ili mijenjanja informacija,

- proceduralna bezbjednost – podrazumijeva odgovor u slučaju incidenta, a menadžment rizika bavi se procjenom balansa bezbjednosnog sistema u odnosu na identifikovanu prijetnju i ranjivost sistema.

Na primjer, prema [ERY02], zaključuje se da je osnovni problem informacione bezbjednosti – ponašanje zaposlenih. Naime 65% od svih napada na sistem bilo je od sopstvenih službenika.

Prema [FBI01], opet slične konstatacije. Problem koji je signiran odnosi se, prije svega, na ponašanje zaposlenih. Naime, 49% detektovanih neautorizovanih pristupa sistemu bilo je, takođe, od zaposlenih u sistemu.

Interesantna su dva, logično suprotstavljena stava, prema [IBM85]. Naime, prema tom pregledu[7], vidi se da je zanemarljiv problem ponašanje kadrova u informacionom sistemu. Ovakvi stavovi su sasvim logični. Ko će da prizna, pa i u anonimnoj anketi, da su mu zaposleni nekompetentni, neobučeni i/ili skloni kriminalu!?

Međutim, prema analizi [IBM85], koju je objavio IBM, spisak uzroka degradacije IS izgledao je ovako:

- greške i propusti, u 50% do 80% svih slučajeva,
- zloupotrebe,
- vatra,
- zlonamjerne štete,
- voda i
- ostalo.

Primijeti se razlika na štetu, tzv. ljudskog faktora, u IBM analizi. Ova razlika je shvatljiva zbog zaštite imidža firme.

Grupa inženjera, u kojoj je bio autor, još je 1999. godine sačinila listu – „*Check Table*" sa oko 160 pitanja. Pitanja su grupisana po faktorima – „sferama" informacione bezbjednosti. Svako pojedinačno pitanje bilo je ponderisano sa 6 do 10 poena. Kompletna tabela može da se vidi u knjizi Rodić, Đorđević, „*Da li ste*

[7] Izveštaj *National Computing Centera* iz Velike Britanije

sigurni da ste bezbedni?".

Slično istraživanje sprovela je i koautorka u okviru doktorske teze „Zaštita i bezbjednost informacija u elektronskoj upravi".

Njeno istraživanje je doprinijelo da se sagleda stanje informacione bezbjednosti i bezbjednosti informacionih sistema u najznačajnijem dijelu republičke i lokalne vlasti, te koliko se ovom veoma značajnom problemu poklanja pažnje, kao i da se ukaže na to šta treba preduzeti da se informaciona bezbjednost u republičkim organima uprave i jedinicama lokalne samouprave u Republici Srpskoj unaprijedi.

Faktori – sfere informacione bezbjednosti su tada bili identifikovani po sljedećem:

- kadrovi,
- normativi,
- organizacione mjere zaštite,
- fizička zaštita,
- zaštita softvera,
- zaštita podataka,
- zaštita u mrežnom okruženju,
- zaštita infrastrukture,
- protivpožarna zaštita.

Dodate su još dvije „sfere":

- sistem u osnovi ne smije biti ugrožen zbog izmjena u sistemu,
- zbog (ne)namjernih propusta.

Važno je u ovom momentu uočiti da tada nije bila definisana težinska vrijednost – ponder pojedine sfere. Na ovaj način, svaki od faktora – sfera učestvovao je tada u ukupnoj ocjeni (provjeri) nivoa informacione bezbjednosti ravnopravno. Uslovno je redoslijed faktora determinisao njihovu hijerarhiju, odnosno značajnost.

U okviru sfere Kadrovi, kroz 11 pitanja provjerava se

sposobnost, kompetentnost lica koja rade u informacionom sistemu. Ona treba da obezbijedi zaštitu ljudi, zaštitu sa ljudima i zaštitu od ljudi (u sistemu i van sistema).

Preko Normativne sfere provjeravano je 10 pitanja. Prije svega, važno je da se provjeri da li postoji interni normativ kojim se definišu skupovi preventivnih i sanacionih zaštitnih mjera. Ovaj normativ treba da ima formu plana, kojim se determinišu sve aktivnosti iz domena informacione bezbjednosti. Kontrolom se provjerava postojanje i ažurnost normativa koji treba da, bez obzira na savjest i stručnost kadrova, obezbijede potpuno i konzistentno sprovođenje svih mogućih mjera zaštite, koje će garantovati najveći mogući nivo informacione bezbjednosti.

Sfera Organizacije provjerava se kroz 24 pitanja. Ova sfera (faktor) treba obezbijediti da se kroz organizaciju, definisanjem timova, nadležnosti (prava i obaveza), u skladu sa normativima, sprovode sve definisane mjere zaštite.

Sfera Fizičke zaštite provjerava se kroz 8 pitanja. Ova sfera „fizički" obezbjeđuje sistem. Putem mnogobrojnih, različitih sistema, od zaštite perimetra, ograda raznih vrsta, zaključavanjem, pristupnim kontrolama, autentifikacijom i autorizacijom, prevenira se neovlašćeni pristup resursima sistema.

Zaštita softvera provjerava se kroz 14 pitanja. Samo pouzdan softver garantuje i pouzdano funkcionisanje sistema. Poseban problem je (ne)poštovanje *copyright* prava – neovlašteno (bez naknade) korištenje softvera, koji se tretira kao autorsko djelo.

Zaštita podataka provjerava se kroz 18 pitanja. Podaci su „srž" informacionog sistema. Mjere zaštite garantuju da se podaci ne mogu (ne)namjerno mijenjati, uništavati i/ili otuđivati.

Specifičnost i masovnost primjene računarskih mreža zahtijeva da se primjene posebne mjere zaštite računarske mreže. Ova sfera provjerava se kroz 15 pitanja. Treba primijetiti da je skup pitanja uslovno široko postavljen – bez obzira na primijenjenu tehnologiju. U okvirima ove i prethodne sfere provjerava se i primijenjena kriptozaštita.

Infrastrukturu informacionog sistema čini sav hardver,

oprema koja je neophodna za funkcionisanje informacionog sistema. Razne vrste instalacija, elektroenergetskih, vodovodnih, za grijanje, za hlađenje, telefonskih, interfonskih..., takođe čine osnovu za pouzdano funkcionisanje informacionog sistema. Ova sfera se provjerava kroz 16 pitanja.

Konačno, zbog značaja (dimenzije) šteta, pojave tzv. „nepovratnih"[8] gubitaka, koje se jave kao posljedica požara u informacionom sistemu, ovoj „sferi" se pridaje posebna pažnja. Ona se provjerava kroz 11 pitanja.

Da bi se nivo informacione bezbjednosti što bolje ocijenio (do)data su još dva pitanja: 1. Sistem ne smije biti ugrožen zbog raznih promjena u sistemu. Doduše, ovo pitanje moglo je da se razmatra i u okviru organizacione sfere[9]. I, 2. Propusti. Broj i vrsta, naročito namjernih propusta, daju potpuniju sliku o nivou informacione bezbjednosti u informacionom sistemu.

3.2. Kako kontrolisati

Uz podrazumijevajuće uslove za kontrolu: dovoljan broj stručnih ljudi, vrijeme, novac..., kontrola se realizuje preko liste pitanja. Svako pojedinačno pitanje se ocjenjuje kako je dato u tabeli. Nakon ocjenjivanja izračunavaju se ocjene za svaku pojedinačnu sferu, kao prosta aritmetička sredina. Nakon toga, na osnovu pondera, slika 2, za svaku pojedinačnu sferu računa se zaključna ocjena kao vagana (ponderisana) aritmetička sredina.

Pitanje	Ocjena	Ponder	(2. * 3.)	Ponderisana ar. sredina
1.	2.	3.	4.	5.
1. Kadrovi	2,64	10,00	26,40	
2. Normativi	4,72	5,00	23,60	
3. Organizacija	6,35	7,00	44,45	

[8] Nepovratni gubici su oni koji se ne mogu povratiti. Prije svega, ljudski životi, kao i ostali resursi IS.

[9] Pažljiviji čitalac može da primijeti da je prisutna nedisjunktnost zaštitnih sfera. Ova činjenica je opravdana i pozitivna upravo u smislu potpunosti i konzistentnosti primijenjenih zaštitnih mjera u sistemu informacione bezbjednosti.

4. Fizička zaštita	5,50	5,00	27,50	
5. Zaštita softvera	6,00	10,00	60,00	
6. Zaštita podataka	8,17	10,00	81,70	
7. Zaštita mreže	3,41	7,00	23,87	
8. Infrastruktura	9,00	9,00	81,00	
9. Promjene	10,00	5,00	50,00	
10. Propusti	9,60	-10,00	-96,00	
	Σ=65,39		Σ= 322,52	$\overline{X}$ = 4,93

Slika 2. Konačna tabela[10] ocjena, provjere sistema informacione bezbjednosti

[10] U koloni 2. su stvarne ocjene pojedinačnog faktora bezbjednosti u informacionom sistemu jedne od najvećih banaka u SRJ 1999. godine.

4. ZAKLJUČAK

Prikazani sistem kontrole nivoa informacione bezbjednosti jeste nezavršen i nesavršen. Prvi je problem identifikacija faktora – sfera sistema informacione bezbjednosti. Prikazani faktori su rezultat kompromisa – usaglašavanja grupe inženjera. Ovo znači da bi neka druga grupa vjerovatno definisala neke druge faktore. Međutim, jednostavno možemo zaključiti da kontrolisano znači – bezbjedno.

Prikazani sistem omogućuje potpunu i konzistentnu kontrolu.

Tehnika i tehnologija ne mogu zamijeniti, ali mogu bitno olakšati organizovanje i sprovođenje informacione bezbjednosti. Težište bezbjednosti mora biti na: preventivi (kroz razvijanje svijesti o opasnostima), osposobljavanju ljudi (da ih prepoznaju, neutrališu, ili smanje rizike); na selekciji ljudi i definisanju pravila bezbjednosnog ponašanja; stalnom preispitivanju uočenih opasnosti i rizika njihovog nastanka, te izradi upotrebljivih i držanju ažurnih planova za ublažavanje rizika i otklanjanje posljedica.

Nijedan sistem nije potpuno usavršen, svaki ima neke slabe tačke, pa možemo zaključiti da apsolutne bezbjednosti informacionog sistema nema. Zapravo ona je apsolutna samo za one sisteme koji – ne postoje. Prema tome apsolutna bezbjednost ne postoji. Sa druge strane, bezbjednost je kao i sreća, nikad potpuna i nikad savršena. Zbog toga cilj bezbjednosti informacionog sistema je da korisnik, neprestano suočen sa potencijalnim opasnostima, upravlja rizikom u radu informacionog sistema, odnosno da utvrđuje, kontroliše i svodi na minimum ili eliminiše opasnosti po sigurnost, koje mogu imati uticaj na informacione sisteme, uz prihvatljivu cijenu.

LITERATURA

[Hsi82] Hsiao D.K, Kerr D.S, Madnik S.E, *Computer security*, Academic Press, New York, San Francisco, London 1979 – ruski prevod Сяо Д, Кэрр Д, Мэдник С, *Защита ЭВМ*, Мир, Moskva 1982.

[Int04] Internet prezentacija, Interpol, *IT security and crime prevention methods* 2004.

[ERY02] EY, Information Security Survey 2001–2002

[FBI01] FBI, Computer Crime and Security Survey, 2001

[How97] Howard D. John, *An Analysis of Security Incidents on the Internet 1989 – 1995*, THESIS – SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY, Carnegie Mellon University – Carnegie Institute of Techology, 1997

[IBM85] IBM – Intertrade, Tehnike osiguranja računskog centra i zaštite podataka, Radovljica,1985.

[Kpm02] KPMG, Global Information Security Survey, www.kpmg.ru 2002.

[Muf79] Muftić Sead, *Sigurnost kompjuterskih sistema*, Zavod za ekonomsko planiranje, Sarajevo 1979. godine,

[Rod04] Boško Rodić, Goran Đorđević*, Da li ste sigurni da ste bezbedni*, Produktivnost A. D, Beograd, 2004.

[RZS02] Republički zavod za statistiku, *Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji, 2009*, Beograd, 2009.