**Dr Boško Rodić,**
pukovnik, dipl. inž.
Uprava za vezu i informatiku GŠ VSCG,
Beograd
**mr Dejan Vuletić,**
kapetan I klase
Institut ratne veštine MO,
Beograd

# SPOSOBNOST OPSTANKA INFORMACIONIH SISTEMA

UDC: 004.382 : 004.052.2

*Rezime:*

*U radu je opisan značaj i trend razvoja informacionih sistema u savremenom društvu, a definisani su i drugi značajni pojmovi radi boljeg razumevanja problema. Prikazana su i četiri aspekta rešenja sposobnosti opstanka informacionih sistema koje predlaže Computer Emergency Response Team (CERT).*

*Ključne reči: informacioni sistem, sposobnost opstanka, napad.*

## SURVIVABILITY OF INFORMATION SYSTEMS

*Summary:*

*The article deals with importance and trend of information systems in modern society. In the article are defined, beside survivability, other relevant ideas necessary for better understanding of the problems. Also, in the article are illustrated four aspects of information system survivability solution by Computer Emergency Response Team (CERT).*

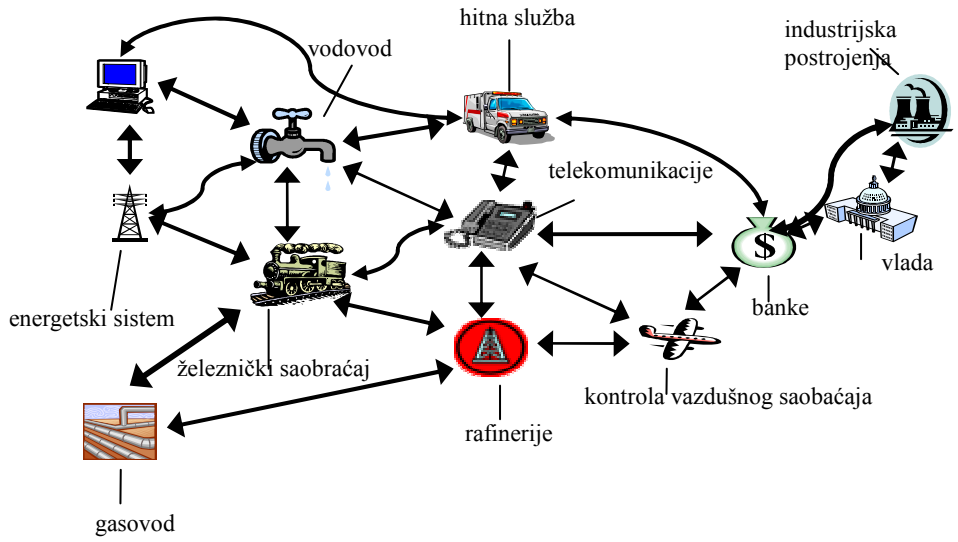
*Key words: information system, survivability, attack.*

## Uvod

Ako se informacioni sistem posmatra kao sistem u kojem se „veza između elemenata sistema ostvaruje razmenom informacija“, (ne)predviđeni događaji, a naročito rat, mogu mu naneti nepopravljive štete, pre svega prekidom informacionih tokova. Na primer, magnetne bure, kao posledica pojačane Sunčeve aktivnosti, slabe ili prekidaju satelitetske veze. Agresija na SRJ 1999. godine započeta je masovnim udarom po komunikacionom sistemu Vojske Jugoslavije, ali je on preživeo i bio u funkciji svih 78 dana neprestanog bombardovanja.

Poseban problem jeste što se zbog ubrzanog razvoja informacione tehnologije i nezaustavljivog rasta njene primene u svim sferama ljudskog društva uvećava njegova ranjivost i izloženost vrlo ozbiljnim potencijalnim opasnostima. Zbog kritičnih tačaka (slika 1), kao i zbog naglašene kompleksnosti i čvrste međuzavisnosti, nacionalne infrastrukture koje povezuju, pokreću i opslužuju računari, postale su izuzetno osetljive i, ako se organizovano napadnu, može da se izazove znatan poremećaj ili destrukcija.

Uspeh svih organizacija zavisi od dostupnosti i pravilnog funkcionisanja širokog spektra složenih informacionih sistema. Zbog ozbiljnih posledica neuspeha organizacije se fokusiraju na sposobnost opstanka sistema, kao na ključni korak upravljanja rizikom.




*Sl. 1 – Kritične tačke nacionalne infrastrukture*

U poslednje vreme najčešće se govori o pojmovima bezbednosti i/ili sposobnosti opstanka računarskih mreža [1, 2]. Međutim, na primeru sposobnosti njihovog opstanka težište će biti na širem pojmu – sposobnosti opstanka informacionog sistema.

## Mogućnosti opstanka informacionih sistema

Uvećana osetljivost informacionih sistema jeste jedan od uzroka povećanog broja incidenata, od kojih mnogi zbog različitih razloga ostaju neobjavljeni. Ipak, korisnici su sve svesniji rizika zbog ranjivosti sistema i cene u slučaju, recimo, gubitka podataka. Nekada je glavna preokupacija korisnika i onih koji izgrađuju informacioni sistem bila – kako učiniti da sistem radi brže i efikasnije, dok je danas glavna preokupacija kako da sistem radi sigurnije.

Današnji informacioni sistemi su sve više povezani u „neobaveznu“ mrežu [1]. Neobavezna, fakultativna ili opciona mreža, na primer Internet, jeste mreža u kojoj ne postoji čvrsta formalna (zakonodavna), organizaciona, pa ni tehnološka međuzavisnost. U ovakvoj mreži u isto vreme dešavaju se dva velika trenda.

Prvi je da pojedinci i organizacije postaju kritično zavisni od ovakvih sistema, a drugi, ranjivost (mrežnih) sistema se naglo povećava zbog toga što sve više potencijalnih napadača ima pristup mreži i tuđim sistemima.

Informacioni sistemi poboljšavaju efikasnost i efektivnost organizacije primenom novih nivoa organizacione integracije. Takve integracije praćene su povišenim nivoom rizika od upadanja u sistem i kompromitovanjem. Ovi rizici mogu biti ublaženi udruživanjem pojedinačnih mogućnosti za opstanak u organizacione sisteme.

Informacioni sistemi bili su i ostali kritični segment ljudskog društva. Ekonomski sektor, odbrana, bezbednost, energetika, telekomunikacije, industrijska proizvodnja, finansije i drugo zavise od informacionih sistema koji rade u lokalnim, nacionalnim ili globalnim razmerama. Društvena zavisnost od informacionih sistema uvećava posledice napada, nezgoda i padova, kao i važnost obezbeđivanja sposobnosti njihovog opstanka. Povezanost mrežnih komunikacija povećava njihovu ranjivost, zbog veće mogućnosti pristupanja informacionoj strukturi iz raznih krajeva sveta.

Većina današnjih istraživanja u oblasti sposobnosti opstanka informacionih sistema usmereno je na odbranu od, pre svega, informacionih upada, što je ograničen pristup jer se usredsređuje skoro isključivo na ojačavanje sistema (npr. korišćenjem firewalla i dr.) da bi se sprečio upad. Za kradljivca, kome je naloženo da se domogne važnih informacija, „ne postoji tehnologija koja može da spreči napad na informacije“ [10]. Prema tome, jedini efikasan način da se umanji pretnja „od krađe podataka“ jeste korišćenje bezbednosne tehnologije u sprezi sa bezbednosnim pravilima u kojim su definisani postupci zaposlenih, kao i sa odgovarajućim obrazovanjem i obukom.

Trend u mrežnim okruženjima informacionih sistema je težnja ka velikim otvorenim mrežnim infrastrukturama. Zatvoreni sistem je onaj u kojem su svi sistemski delovi kontrolisani jedinstvenom upravom i mogu biti kompletno određeni i kontrolisani, čak su i fizički odvojeni od otvorenih mrežnih infrastruktura. U otvorenim sistemima ne postoji jedinstvena uprava nad njegovim delovima. Termin uprava (administrativna kontrola) predstavlja moć da se određuje i primorava sankcijama, a ne da se jednostavno preporuči prikladna bezbednosna politika. U otvorenom sistemu svaki učesnik se mora osloniti i verovati informacijama koje pristižu iz okruženja, i ne može vršiti kontrolu izvan svog lokalnog područja.

Uprkos naporima onih koji se bave bezbednošću, nijedan stepen jačanja sistema ne može sa sigurnošću obezbediti da sistem koji je priključen na otvorenu mrežu bude neranjiv na napade. Disciplina sposobnosti opstanka informacionih sistema može pomoći da se obezbedi da takav sistem radi sa osnovnim servisima i da održava osnovne osobine, kao što su [6]:

– poverljivost,
– integritet,
– raspoloživost,
– pouzdanost,
– neporecivost informacija (podataka),
– proverenost,

uprkos, recimo, prisutnim upadima. Za razliku od tradicionalnih bezbednosnih mera koje zahtevaju centralnu komandu ili administraciju, sposobnost za opstanak je namera da se spozna, recimo, otvoreno mrežno okruženje.

*Napadi* su slučajevi potencijalnog oštećivanja informacionog sistema, kojim upravljaju napadači. Napadači mogu da se svrstaju u sledećih šest kategorija [3, 6]: 1) hakeri – „provaljuju“ u računar prvenstveno zbog izazova radi statusa prioritetnog korisnika sistema; 2) špijuni – „provaljuju“ u računar prvenstveno zbog informacija koje se mogu upotrebiti za političku dobit; 3) teroristi – „provaljuju“ u računar radi izazivanja straha koji im omogućava političku dobit; 4) korporacijski napadači – osoblje jedne

kompanije „provaljuje“ u informacione sisteme druge kompanije radi finansijskog dobitka; 5) profesionalni kriminalci – „provaljuju“ u informacione sisteme zbog ličnog finansijskog dobitka; 6) vandali – „provaljuju“ u informacione sisteme prvenstveno radi nanošenja materijalne štete.

Međutim, uočava se nepotpunost navedene klasifikacije [6]. Naime, ni u jednoj od šest kategorija nisu spomenute „štetočine“ (insajderi) – zaposleni u informacionom sistemu: službenik analfabeta, službenik ljubitelj – „istraživač“ (diletant) i unutrašnji zlonamernik.

Napad se sastoji od upada, proba i obaranja sistema [1].

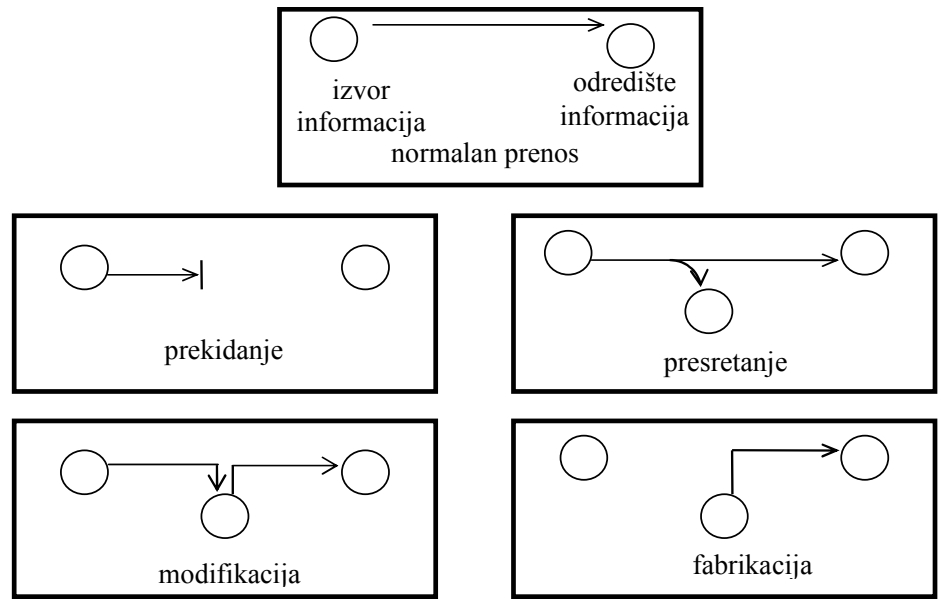
*Incident* čini grupu napada koja se može razlikovati od ostalih napada po prepoznatljivosti napadača, stepenu sličnosti sajtova, tehnika i drugo. Napad se definiše i kao „serija namernih koraka preuzeta od strane napadača da bi postigao neautorizovan rezultat“. Upad predstavlja kombinaciju *(alat + akcija + meta)*.

*Nezgode* predstavljaju širok spektar slučajno iskrslih i potencijalno štetnih događaja, kao što su prirodne nepogode.

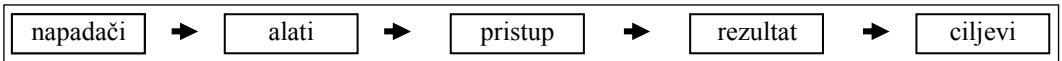
*Padovi sistema* su mogući štetni događaji prouzrokovani manjkavostima u sistemu ili u spoljnim elementima od kojih sistem zavisi. Padovi sistema prouzrokovani su greškama u izradi softvera, zastarevanju hardvera, ljudskim greškama, itd.

## Primeri ugrožavanja informacionih sistema

Stolings predlaže jednostavan model koji klasifikuje pretnje informacionim sistemima [6]. Model se odnosi samo na podatke u tranzitu. Uočavaju se četiri kategorije (slika 2): 1) prekidanje – resursi sistema su uništeni ili nedostupni korisnicima; 2) presretanje – neovlašće-




*Sl. 2 – Klasifikacija napada na informacije po Stolinsu*




*Sl. 3 – Sekvenca napada po Hauardu*

no lice pristupa resursima sistema; 3) modifikacija – neovlašćeno lice ne samo da pristupa resursima sistema već ih i modifikuje i 4) fabrikacija – neovlašćeno lice unosi falsifikovane objekte u sistem. Presretanje predstavlja pasivan napad, dok su prekidanje, modifikacija i fabrikacija aktivni napadi [4].

Prema Hauardu napadač na informacioni sistem pokušava da dostigne vezu krajnjeg cilja i motiva [3]. Ova veza se može opisati sekvencom koju čine alati, pristup i rezultati napada, kao što je prikazano na slici 3.

Svako oštećenje, promena i/ili uništenje informacija u informacionom sistemu, predstavlja degradaciju informacionog sistema [5].

## Mere sposobnosti opstanka informacionih sistema

Otvoreni sistemi su značajna komponenta u današnjem informacionom okruženju, a u budućnosti će imati još značajniju ulogu. Internet – mreža sistema bez hijerarhije (ustrojstva), od kojih je svaki isključivo pod svojom lokalnom administrativnom kontrolom, osnovni je primer otvorenog sistema. Dok konvencije postoje da bi dozvolile delovima Interneta da međusobno funkcionišu, ne postoji globalna administrativna kontrola koja treba da obezbedi da se ovi delovi ponašaju shodno konvencijama. Zbog toga postoji mnogo problema. Na žalost, sposobnost opstanka otvorenih sistema najčešće je potcenjena.

Otvoreni sistem može biti sačinjen od zatvorenih i otvorenih sistema povezanih u mrežu. Na slici 4 prikazano je otvoreno područje koje se sastoji od više zatvorenih sistema, kod kojih je svaki pod različitom upravom. Iako bezbednosna politika pojedinačnog zatvorenog sistema ne može biti kompletno primorana na nešto od nekog izvan granica njegove administrativne kontrole, ona može biti realizovana radi obezbeđenja stanja bezbednosti tog zatvorenog sistema. Naravno, bezbednosna politika može biti predočena javnosti, ali administratori su višestruko ograničeni u svojoj mogućnosti da prisile ili ubede pojedince i celine da je slede.

*Sposobnost opstanka informacionog sistema* definiše se kao mogućnost sistema da ispuni svoju misiju i pored prisutnih napada, padova sistema i nezgoda. Termini napad, pad sistema i nezgoda predstavljaju potencijalne štetne događaje. Termin sistem u najširem smislu, uključuje i računarske mreže [1]. Sposobnost opstanka informacionog sistema definiše se i kao „sposobnost sistema da se oporavi od napada i nivoa do kojeg se oporavio“ [2].

Ključna osobina sposobnosti opstanka informacionih sistema je njihova sposobnost da održe osnovne servise tokom napada, pada sistema ili nezgode. Zato je vrlo bitno odrediti minimalni nivo kvalitativnih svojstava koji je povezan sa nekim osnovnim servisom. Ova kvalitativna svojstva toliko su bitna da su definicije sposobnosti za opstanak često izražene kao održavanje balansa između drugih kvalitativnih svojstava, kao što su performanse, tolerancija nedostataka, sposobnost izmena i korisnost.

Dakle, povezana je mogućnost sistema da vremenom ispuni svoju misiju sa njegovom sposobnošću da održi osnovne servise u slučaju napada, nezgode ili pada sistema. Obavezno mora opstati izvršenje misije, a ne neki deo ili komponenta sistema. Ako je, ipak, osnovni servis izgubljen, on može biti zamenjen drugim servisom koji obezbeđuje izvršenje misije na drugačiji, ali ekvivalentan način.

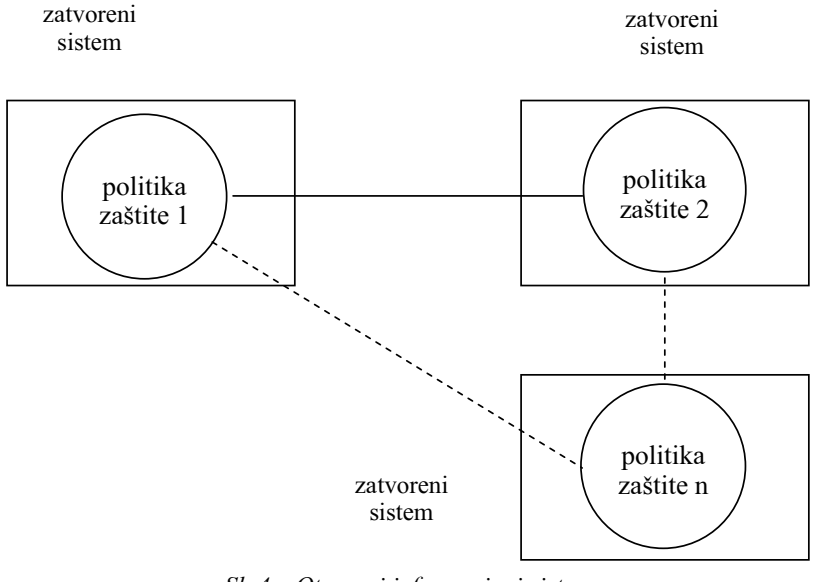
Da bi održali njihovu sposobnost sprovođenja osnovnih servisa [1], sistemi sposobni za opstanak moraju imati četiri ključna svojstva prikazana u tabeli 1.

Termin misija odnosi se na skup (apstraktnih) zahteva ili ciljeva vrlo visokog nivoa. Izvršenje misije znači da ona mora da opstane, a ne neki podsistem ili sistemska komponenta. Ako sistem zadrži integritet i poverljivost svojih podataka i nastavi rad svojih osnovnih servisa posle prolaska perioda problema u okruženju, može se reći da je ispunio svoju misiju.

Računarska mreža, na primer, kao infrastrukturna osnova informacionog sistema obezbeđuje se radi zaštite resursa informacionog sistema, od mogućih prolaznih ili trajnih oštećenja, uništenja ili bilo kakvih štetnih događaja koji bi mogli ugroziti njen rad.

Da bi informacioni sistem opstao, on mora da reaguje ili se oporavi od štetnih efekata mnogo pre nego što se otkrije pravi razlog tih efekata. U stvari, reagovanje i oporavak moraju biti uspešni bez obzira na to da li je uzrok otkriven.

Mogućnost opstanka zavisi od tri ključne sposobnosti: otpora, prepoznavanja i oporavka (Resistance, Recognition and Recovery). Otpor je sposobnost sistema da odbije napade. Prepoznavanje je sposobnost otkrivanja napada kada se pojave, i procena razmera štete. Oporavak, reper za sposobnost opstanka, jeste sposobnost održavanja osnovnih usluga i dobara tokom napada, ograničavanja štete i ponovno uspostavljanje svih usluga nakon napada [1].




*Sl. 4 – Otvoreni informacioni sistem*

*Tabela 1*

*Osobine sistema sposobnih za opstanak*

| Ključna osobina | Opis mera | Primer mera |
|---|---|---|
| Otpomost na napade | Strategije za odbijanje napada | Identifikovanje korisnika. Korišćenje različitih programa |
| Prepoznavanje napada i obima oštećenja | Strategije za prepoznavanje napada (uključujući i upade) i razumevanje trenutnog stanja sistema, uključujući i procenjivanje obima oštećenja. | Unutrašnja provera integriteta (celovitosti) |
| Oporavak potpunih i osnovnih servisa posle napada | Strategije za povraćaj kompromitovanih informacija ili funkcionalnosti, ograničenje obima oštećenja, održavanje ili, ako je potrebno, povraćaj osnovnih servisa u ograničenom roku misije, povraćaj potpunih servisa, kako to uslovi dozvoljavaju. | Dupliranje i ponovno vraćanje podataka na početno stanje. |
| Adaptacija i razvoj radi sprečavanja efikasnosti budućih napada | Strategija za poboljšanje sistemske sposobnosti za opstanak, a koje se zasniva na prethodnim iskustvima sa upadima. | Udruživanje u novi model za prepoznavanje upada |

*Tabela 2*

*Aspekti sposobnosti za opstanak*

| Aspekti sposobnosti za opstanak | Navodi strategija |
|---|---|
| Otpor | – tradicionalna bezbednost, uključujući kriptovanje i skrivene kanale<br>– raznolikost i uvećane razlike u pojedinačnim čvorovima<br>– analitičke rezerve i glasanje<br>– specijalizacija, podela rada, poverenje i informacije<br>– neprestano potvrđivanje nadzora<br>– pokazana svojstva na osnovu pretpostavki i slučajno ponašanje |
| Prepoznavanje | – analitička suvišnost i testiranje (uključujući greške u softveru, kriptovanje i nadzor)<br>– nadgledanje upada i sumnjivih aktivnosti<br>– ponašanje sistema i nadgledanje celovitosti |
| Oporavak | – fizičke i informacione rezerve<br>– nelokalne kopije informacionih resursa<br>– pripreme, spremnost, slučajno planiranje i timovi za odgovor |
| Prilagođavanje i evolucija | – sveopšte ili određene izmene radi otpora, prepoznavanja ili oporavka od ranjivosti koje su otkrivene<br>– slanje upozorenja ostalim čvorovima<br>– objavljivanje strategija prilagođenja i evolucije<br>– zastrašivanje kroz odmazde i kazne |

Kao što je predstavljeno u tabeli 2, CERT predlaže četiri aspekta rešenja koja mogu služiti kao osnova za strategiju sposobnosti za opstanak.

## Pouzdanost i raspoloživost informacionih sistema u funkciji sposobnosti opstanka

Pouzdanost sistema podrazumeva njegovu sposobnost da održava njegovo radno stanje i u reduciranim uslovima okruženja [6].

Pouzdanost uključuje sledeće sposobnosti: 1) nastavljanje rada nakon što neke komponente sistema „ispadnu“ iz rada; 2) održavanje integriteta snimljenih informacija; 3) postojanje rezervnih komponenti i/ili puteva u sistemu; 4) uočavanja „ispada“ neke komponente iz rada; 5) reorganizaciju onih elemenata koji su još u dobrom radnom stanju u modificiranom sistemu.

Pouzdanost sistema je kvalitativna jedinica. Danas ne postoje opšteprihvaćeni kriterijumi za određivanje jedinice kojom bi se mogla meriti veličina pouzdanosti, pa se pouzdanost i ne meri.

Na pouzdanost se može uticati odgovarajućim organizacionim merama. Glavni preduslov za povećanje pouzdanosti sistema su prepreke u slučaju nastupa greške, odnosno „ispada“ komponente iz rada, odnosno preventivne mere.

Preventivne mere, usmerene na povećanje pouzdanosti sistema, obuhvataju:

– planiranje i očuvanje vitalnih podataka, kopiranjem podataka i snimanjem na različitim lokacijama, a u trenutku nastajanja tih podataka, odnosno pre njihovog fizičkog premeštanja i očuvanje integriteta podataka;

– zaštitu vitalnih podataka, zaštitom glavne memorije i zaštitom datoteka i banaka podataka sa spoljnim memorijama;

– razradu strategije ponovnog puštanja u rad (recovery strategy);

– planiranje sistema tako da se smanji međusobna zavisnost pojedinih ključnih komponenti;

– pripremu preventivnih mera kao osnovnog sredstva za povećanje raspoloživosti;

– ugrađivanje sposobnosti sistemske rekonfiguracije u hardver i softver od samog početka planiranja sistema.

Raspoloživost sistema predstavlja matematičku verovatnoću da će sistem, u skladu sa svojim projektovanim performansama, izvršavati određene funkcije u određenom vremenu i pod određenim uslovima [6].

### Rizici u informacionim sistemima

Kako sposobnost opstanka informacionog sistema obavezno uključuje agresiju, može da se zaključi da je:

$$Pr \subseteq B$$

gde je:
$Pr$ – sposobnost opstanka informacionog sistema,
$B$ – bezbednost informacionog sistema.

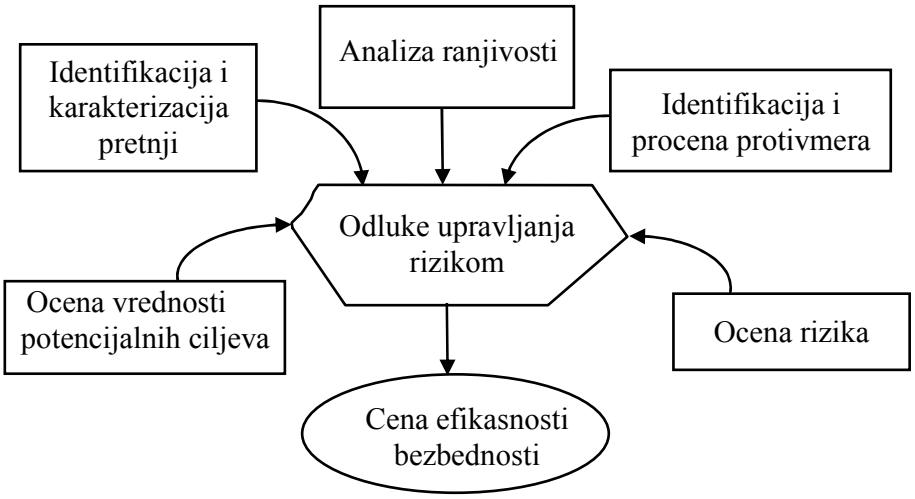
Informacioni sistem ne može biti apsolutno bezbedan [6]. Zato korisnik, suočen sa potencijalnim opasnostima, treba da upravlja rizikom u njegovom radu. To je postupak utvrđivanja, kontrolisanja i svođenja rizika na minimum ili eliminisanja opasnosti po sposobnost opstanka koje mogu imati uticaj na informacione sisteme, uz prihvatljivu cenu [6].

Postoji više načina razmatranja rizika: izbegavanje, zadržavanje, smanjivanje i prebacivanje. Korisnik će, u skladu sa šemom na slici 5, odlučiti kako da upravlja rizikom. Odluka će biti određena sledećom formulom:

$$R = \frac{Pr \cdot Ra \cdot Z}{Pm},$$

gde je:
$R$ – stepen rizika, od 0,1 do 1000;
$Pr$ – stepen pretnji, od 1 do 10;
$Ra$ – stepen ranjivosti sistema, od 1 do 10;
$Z$ – značaj sistema, od 1 do 10;
$Pm$ – intenzitet protivmera, od 1 do 10.

Stepen, ili intenzitet pretnji, mera je frekvencije i snage pretnji. Neke pretnje nikada ne budu otkrivene, pa se angažuju posebne službe koje otkrivaju ili procenjuju mogućnost pretnje. Ranjivost sistema je, u stvari, obrnuto srazmerna stepenu branjenosti sistema. Značaj sistema zavisi od finansijske, materijalne ili političke vrednosti. Analiza pretnji, ranjivosti i značaja sistema pomaže u vođenju i određivanju potrebnih aktivnosti rukovodstva i prioriteta u radu sa rizicima u zaštiti informacija, kao i pri uvođenju kontrola odabranih da bi štitile od tih rizika. Ponekad je potrebno da se postupak ocenjivanja rizika i odabiranja kontrole ponove nekoliko puta, kako bi se obuhvatili razni delovi organizacije ili pojedinačni informacioni sistemi. Metode ocenjivanja rizika mogu se primeniti na celokupnu organizaciju, ili samo na njene delove, kao i na pojedinačne informacione sisteme, specifične komponente sistema ili usluge, kao i funkcije, tamo gde je to izvodljivo.




*Sl. 5 – Proces upravljanja rizikom*

Za imaoce informacionih sistema odluke mogu da budu:

– izbegavati rizik. Privremeno se napuštaju određene funkcije sistema ili se ne koriste neke komponente sistema (hardver ili softver) koje su najugroženije, a bez kojih sistem može, uz manji rizik, da obavlja preostale radne zadatke. Izbegavanje rizika je privremena i svesna degradacija sistema. Ova mera se koristi ako nije na raspolaganju neka druga ekonomičnija i efikasnija mera;

– zadržati rizik. Nakon analize pretnji, ranjivosti sistema i raspoloživih protivmera, prihvata se rizik. Ta mera se koristi kad su pri konkretnom riziku male štetne posledice ili je šteta manja od troškova zaštite;

– smanjiti rizik. Primeniti zaštitne mere moguće je i kao kompromis između troškova zaštite i troškova štete;

– prebaciti rizik. Delimično ili potpuno prebaciti rizik ugovorom o održavanju, osiguranjem u slučaju štete kod osiguravajućeg zavoda i slično.

Potrebno je sprovoditi periodična preispitivanja rizika po bezbednost i uvedenih mera zaštite, kako bi se [6]:

– uzele u obzir izmene u poslovnim zahtevima i prioritetima;

– razmotrile nove pretnje i ranjivosti;

– analizirao sistem u izmenjenim uslovima (hardver, softver);

– potvrdilo da su kontrole ostale efikasne i odgovarajuće.

Preispitivanja treba izvoditi na raznim nivoima dubine, zavisno od rezultata prethodnih ocenjivanja i promenljivog nivoa rizika koje je rukovodstvo spremno da prihvati. Ocenjivanje rizika često se prvo sprovodi na nekom visokom nivou, kao sredstvom za prioritetne resurse u područjima visokog rizika, a zatim na nivou detalja, radi iznalaženja specifičnih rizika.

Kada su zahtevi za bezbednost definisani, treba odabrati i ugraditi kontrolne mere, kako bi se osiguralo da će rizici biti smanjeni na prihvatljiv nivo. Kontrole se mogu odabrati ili se, prema potrebi, mogu projektovati druge kontrole kako bi se zadovoljile specifične potrebe [6].

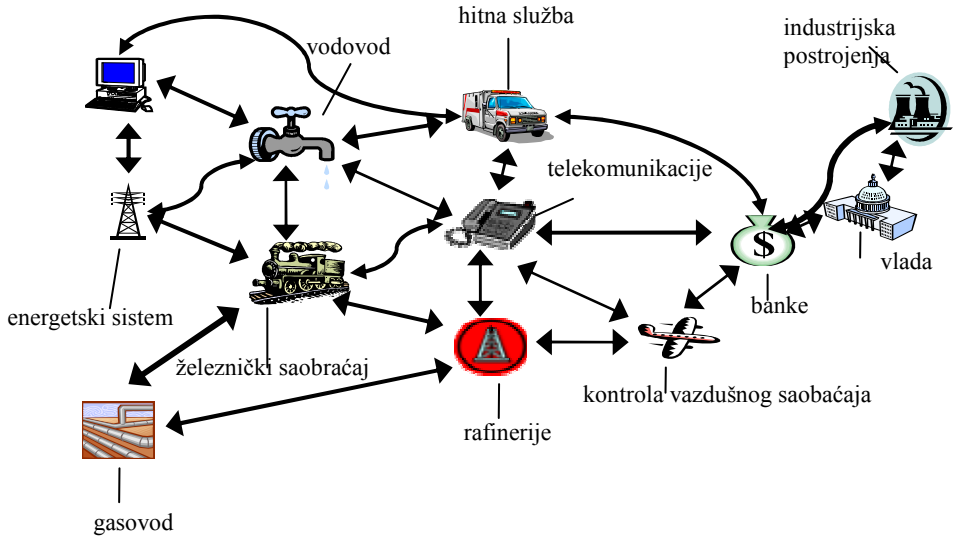
## Zaključak

Informacioni sistemi su veoma ranjivi i izloženi ozbiljnim potencijalnim opasnostima. Rešenje sposobnosti njihovog opstanka veoma je složen problem, čije rešenje zahteva znatno angažovanje svih segmenata društva.

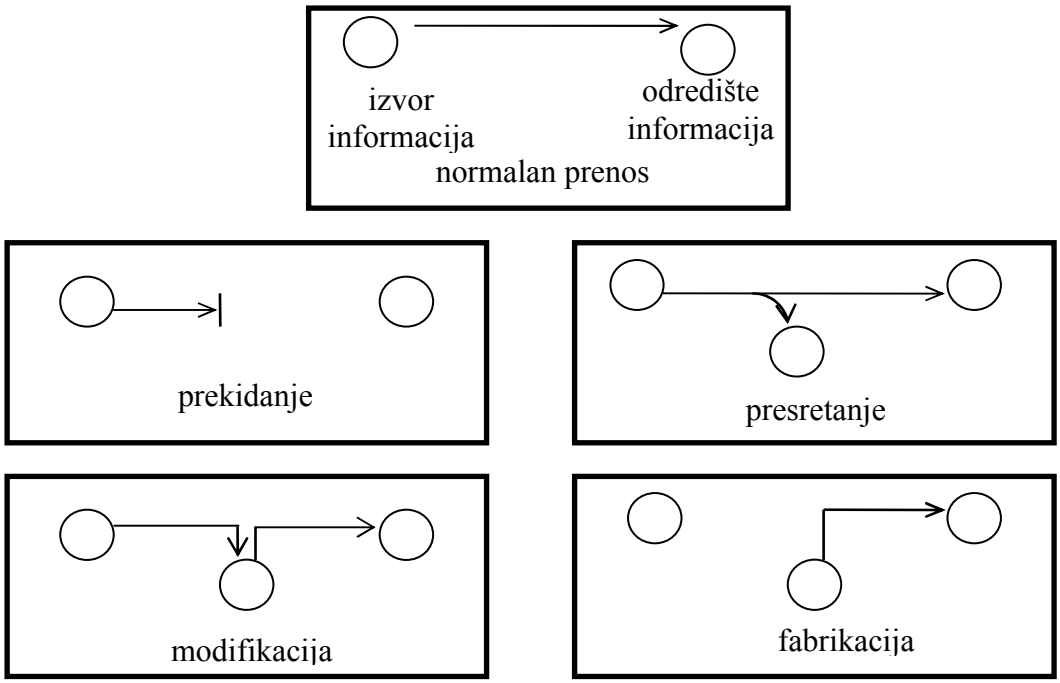
Najslabija karika svakog informacionog sistema svakako je čovek. U vezi s tim, nerealna je apsolutna sposobnost opstanka informacionog sistema ali se rizicima u znatno većoj meri može upravljati.

*Literatura:*

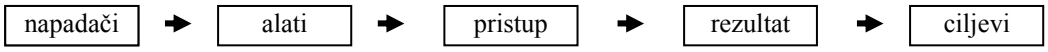

[1] www.cert.org
[2] Ellison, J., Fisher, A.: Survivable Network Systems: An Emerging Discipline, Pittsburgh, Carnegie Mellon University, 1987.
[3] Howard, J.: An Analysis of Security Incidents on the Internet 1989–1995, Ph. D. Dissertation, Carnegie Mellon University – Carnegie Institute of Technology, Pittsburgh, PA, 1995.
[4] Stallings, W.: Network and Internetwork Security Principles and Practice, Prentice Hall, Englewood Cliffs, 1995.
[5] Rodić, B.: Interakcija javnih računarskih mreža i računarskih mreža specijalnih institucija (doktorska disertacija), Vojnotehnička akademija, Beograd, 2001.
[6] Rodić, B., Đorđević, G.: Da li ste sigurni da ste bezbedni, Produktivnost AD, Beograd, 2004.
[7] www.geneva-link.ch/pgalley/infosec/
[8] Munro, N.: The Pentagon's New Nightmare: An Electronic Pearl Harbor, Washington Post 16. 07. 1995.
[9] Washington D. W, Prema kiber vojnicima, magazin TIME, 21. 08. 1995.
[10] Mitnik D. Kevin, Sajmon L. Vilijam, Umetnost obmane, Mikroknjiga, Beograd, 2002.



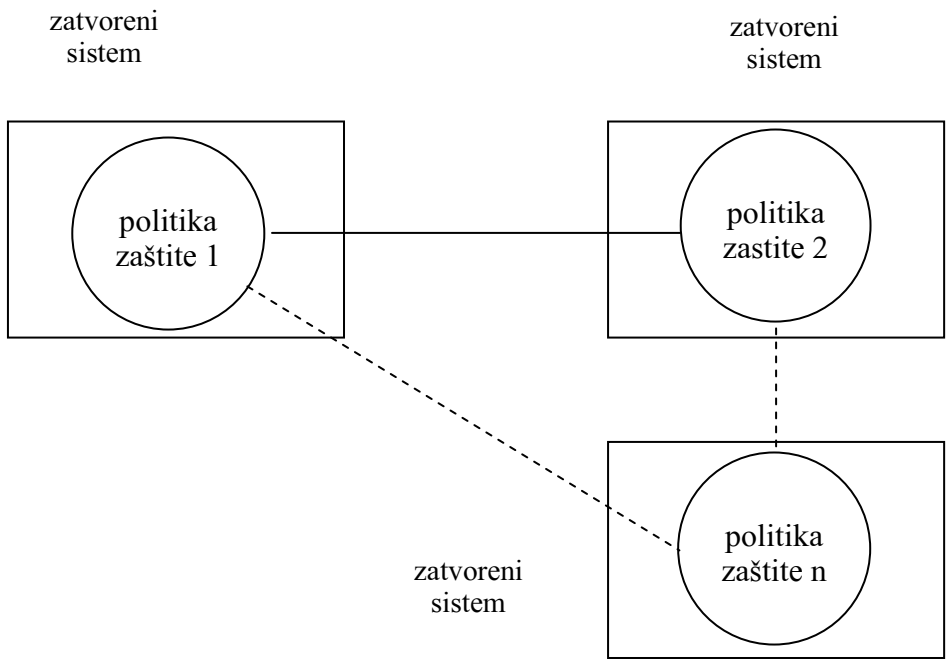

*Sl. 1 – Kritične tačke nacionalne infrastrukture*



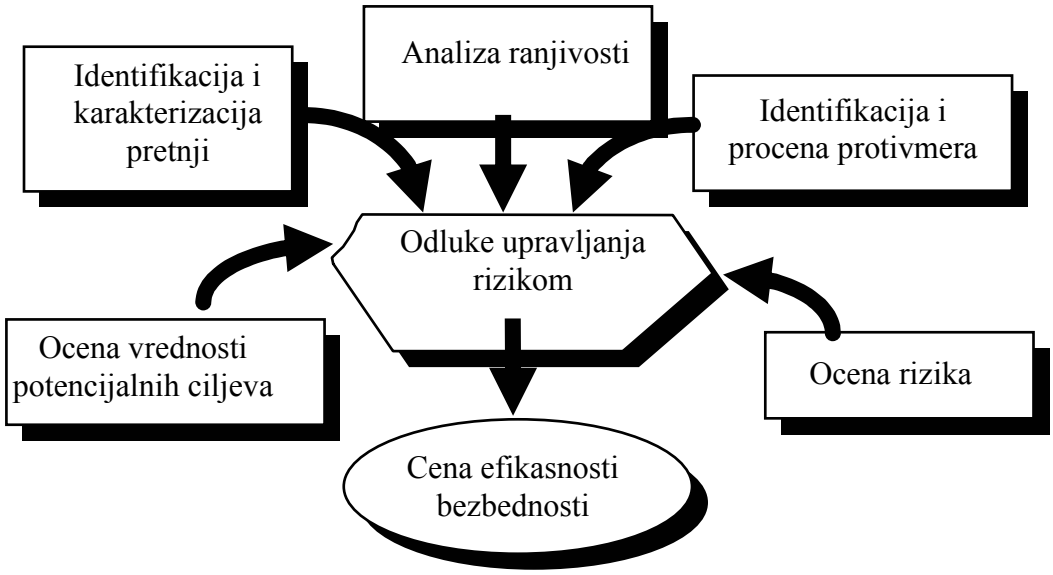

*Sl. 2 – Klasifikacija napada na informacije po Stolinsu*




*Sl. 3 – Sekvenca napada po Hauardu*




*Sl. 4 – Otvoreni informacioni sistem*




*Sl. 5 – Proces upravljanja rizikom*