



TOWERS NET
IT & Telecommunications Innovations



Mr Zoran Živković, dipl.inž
Predsednik Društva za Informativnu bezbednost Srbije

STANJE INFORMACIONE BEZBEDNOSTI SRBIJE

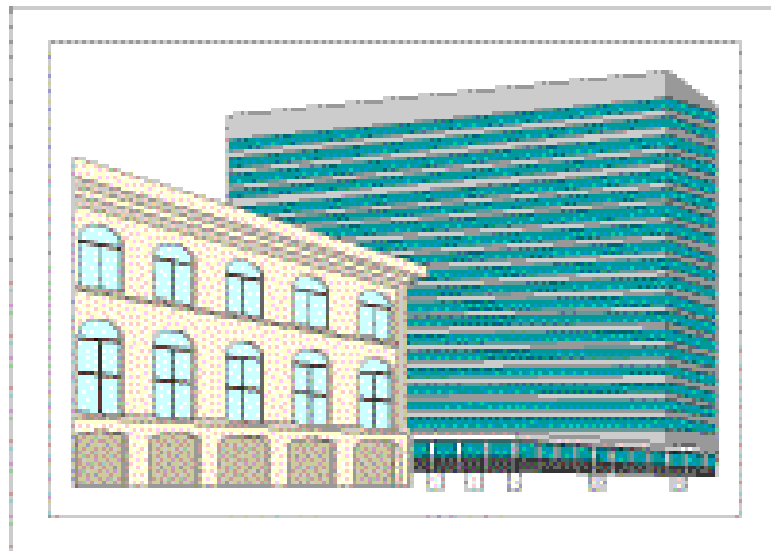
Koautori: Stevan Sinkovski, Milan Živković

1. Stanje informacione bezbednosti u Srbiji

- Konferencija IB 2013:
 - Informaciona bezbednost mora da postane **strateška obaveza Vlade i njenih organa**. "IB mora da bude rangirana visoko na listi prioriteta, i **prva i najvažnija** stvar koja treba da se uradi je donošenje nacionalne strategije o IB" (predsednik programskog odbora DIBS-a, **prof.dr.Slobodan Petrović**).
 - Stanje po pitanju IB u Srbiji je **alarmantno**, jer **ne postoji organizaciona celina na državnom nivou** koja se bavi problemom IB-a, kao ni zvanična vizija potencijalnog rešenja (**pukovnik Ivan Vulić** iz Ministarstva odbrane).
 - **"Nema definisane kritične infrastrukture** - šta treba braniti i sa kojim snagama i resursima kada je u pitanju IB, a samo u toku mesec dana zabeleženo je preko 1700 pojava koje se mogu tretirati kao napad na sajt predsednika Srbije, oko 3800 pokušaja skeniranja sistema, i između 1400 i 4500 pokušaja napada na sajt Vojske Srbije, a do pre par godina nije bilo nikoga ko je nadgledao sajtove" (**pukovnik Vulić**).
 - **Srbija jedna od pet zemalja u Evropi koja još nema svoj CERT** (Computer Emergency Response Team), a postoje velike šanse da do kraja godine bude i jedina, što govori u koliko je lošem stanju Informaciona bezbednost u Srbiji (predsednik DIBS, **mr Zoran Živković,dipl.ing.**).

Zaštita informacija – osnova bezbednog biznisa

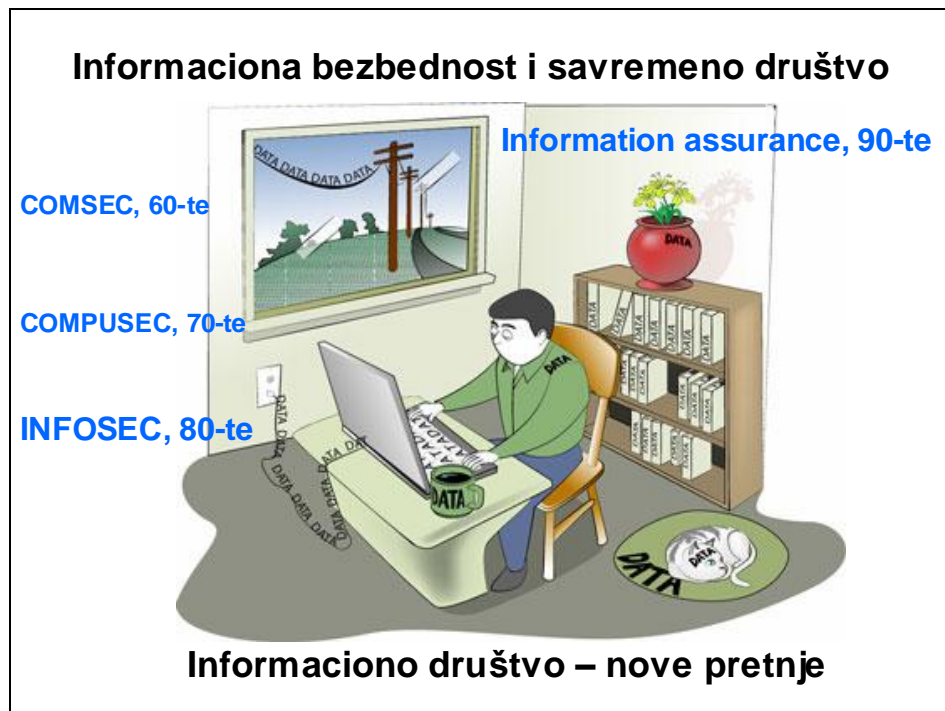
- „Neophodno da se što pre napravi **Strategija Informacione bezbednosti** Srbije u okviru Akcionog plana razvoja IKT društva Srbije, koji je Vlada donela početkom godine”.
- da ukoliko se sprovedu samo **dve od četiri tačke iz Akcionog plana, kao što je formiranje CERT-a i Zakona o IB**, možemo biti zadovoljni (predsednik Društva za Informacionu bezbednost DIBS, mr **Zoran Živković, dipl.ing.**).



2. Informaciona bezbednost u svetu

2.1. Istorijski kontekst i pojam IB

- Informaciona bezbednost 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 mere detekcije, dokumentovanja i otklanjanja takvih pretnji



- Informaciona garancija (IA) je definisana kao «informacione operacije zaštite i odbrane informacija i informacionih sistema obezbeđujući njihovu raspoloživost, integritet, autentičnost, poverljivost i neporicljivost. Ovo podrazumeva restauraciju informacionih sistema inkorporiranim mogućnostima zaštite, detekcije i reakcije»[\[1\]](#).
 - [Evropske zemlje](#), u svom shvatanju pojma informacione bezbednosti, sa naglašenijim pragmatičnim pristupom, prate poglede SAD
 - Informaciona bezbednost je, u doktrinarnim dokumentima RF, definisana kao
 - stanje zaštićenosti životno važnih interesa ličnosti, društva i države u informacionoj sferi od spoljašnjih i unutrašnjih opasnosti (rizika) odnosno kao
 - stanje zaštićenosti informacione sredine društva koje omogućava njeno formiranje, korišćenje i razvoj u interesu građana, organizacija, države.
- [\[1\]](#) Na isti način informaciona garancija je definisana i u rečniku NSTISSC, zajedničkoj doktrini informacionih operacija (JP 3-13, 1998:1-9) i u pravilu KoV-a FM 3-13, 2003. god..

2.2. Aspekti informacione bezbednosti

- Pravni aspekt
 - Savremeno društvo, nastalo na razvoju informacionih tehnologija i procesa globalizacije na ekonomskom planu, zahteva jačanje internacionalne koordinacije (zakonodavstvo na međunarodnom nivou) kao jedinog pristupa koji omogućava pravno regulisanje odnosa u kiber-prostoru i kompjuterskih prestupa
- podrazumeva nekoliko pitanja:
 - pitanje čuvanja i korišćenja **personalnih podataka** (zaštita privatnosti),
 - problem zaštite (tehničkog čuvanja) **masiva podataka** od falsifikata,
 - problem zaštite **autorskih prava**,
 - pitanje pravne **validnosti elektronskih dokumenata** (važnost ugovora),
 - problem zaštite **podataka i žigova**,
 - prava potrošača i
 - pitanja **zloupotrebe kompjuterskih sistema** (zaštita od prevare i organizovanog kriminala) i
 - načina **pravnog sankcionisanja** kompjuterskih prestupa.

Tehnički aspekt IB

Kompromitujuća EM zračenja PC računara

Kanali oticanja informacija

- 1- Materijalna korist
- 2- Nezadovoljstvo
- 3- Neznanje

- 1- Personal
- 2- Tehnički kanali



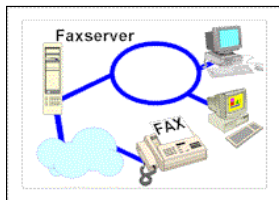
čuvanje podataka

komunikacije

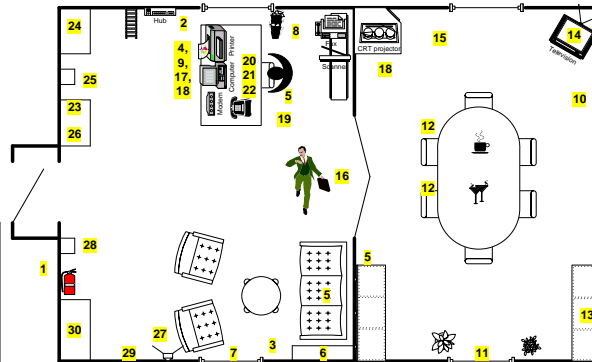


Modem

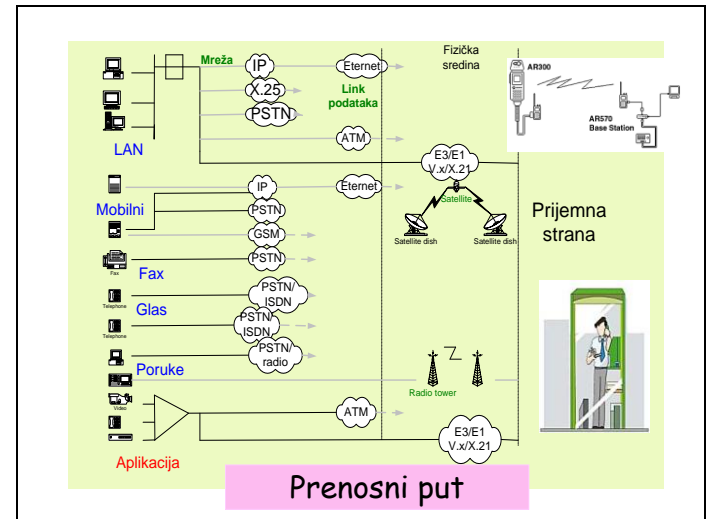
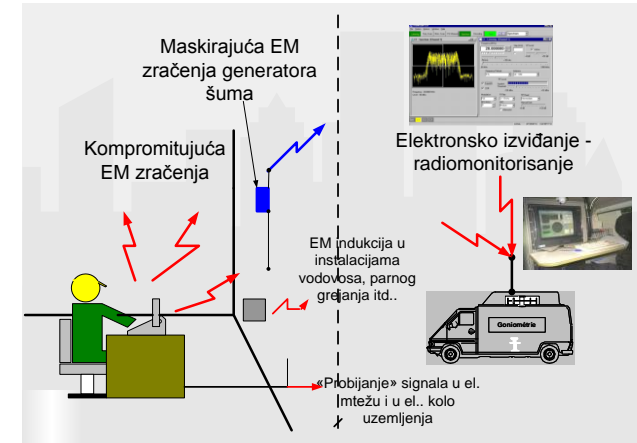
mreže



Faxserver



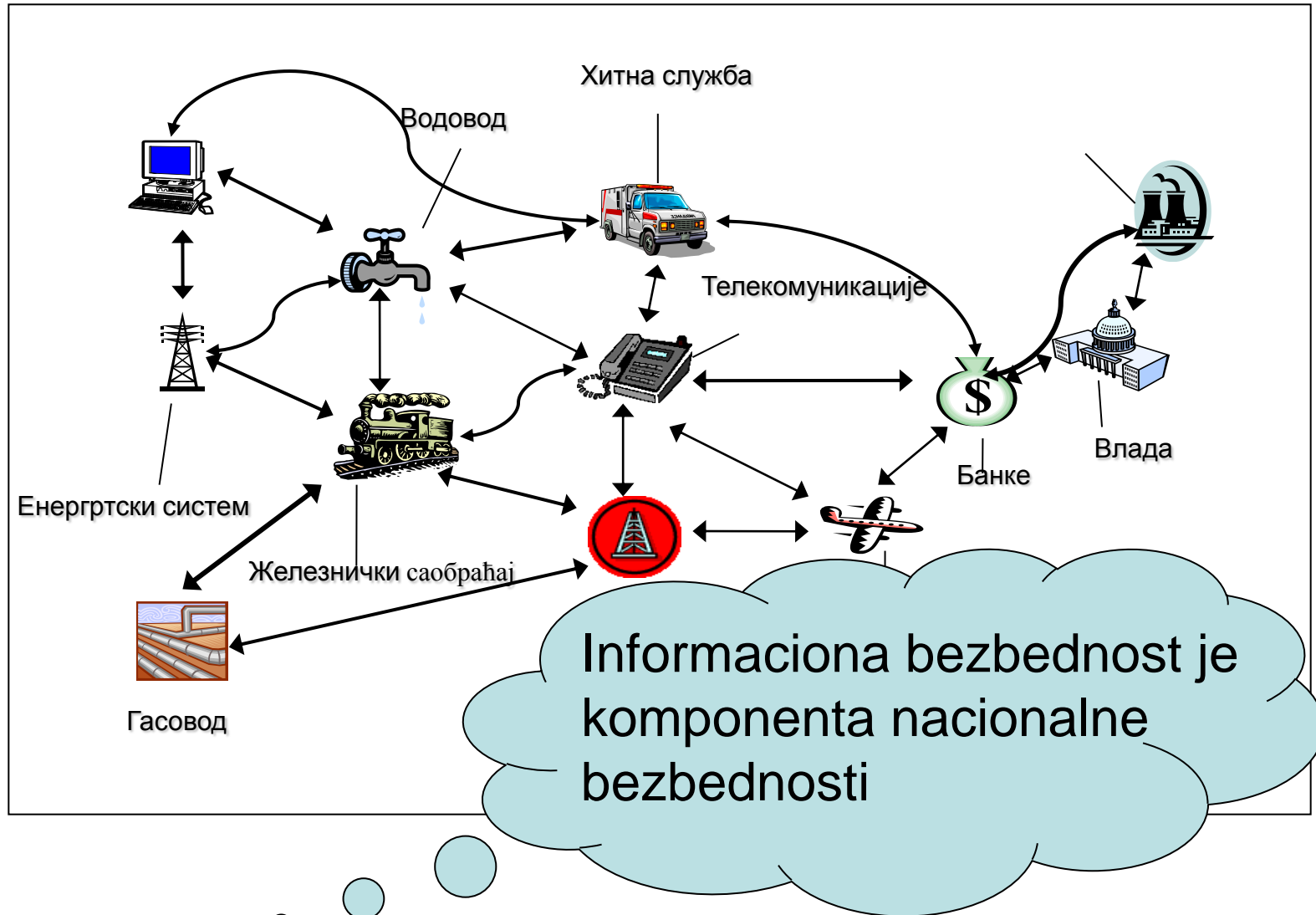
poslovne prostorije

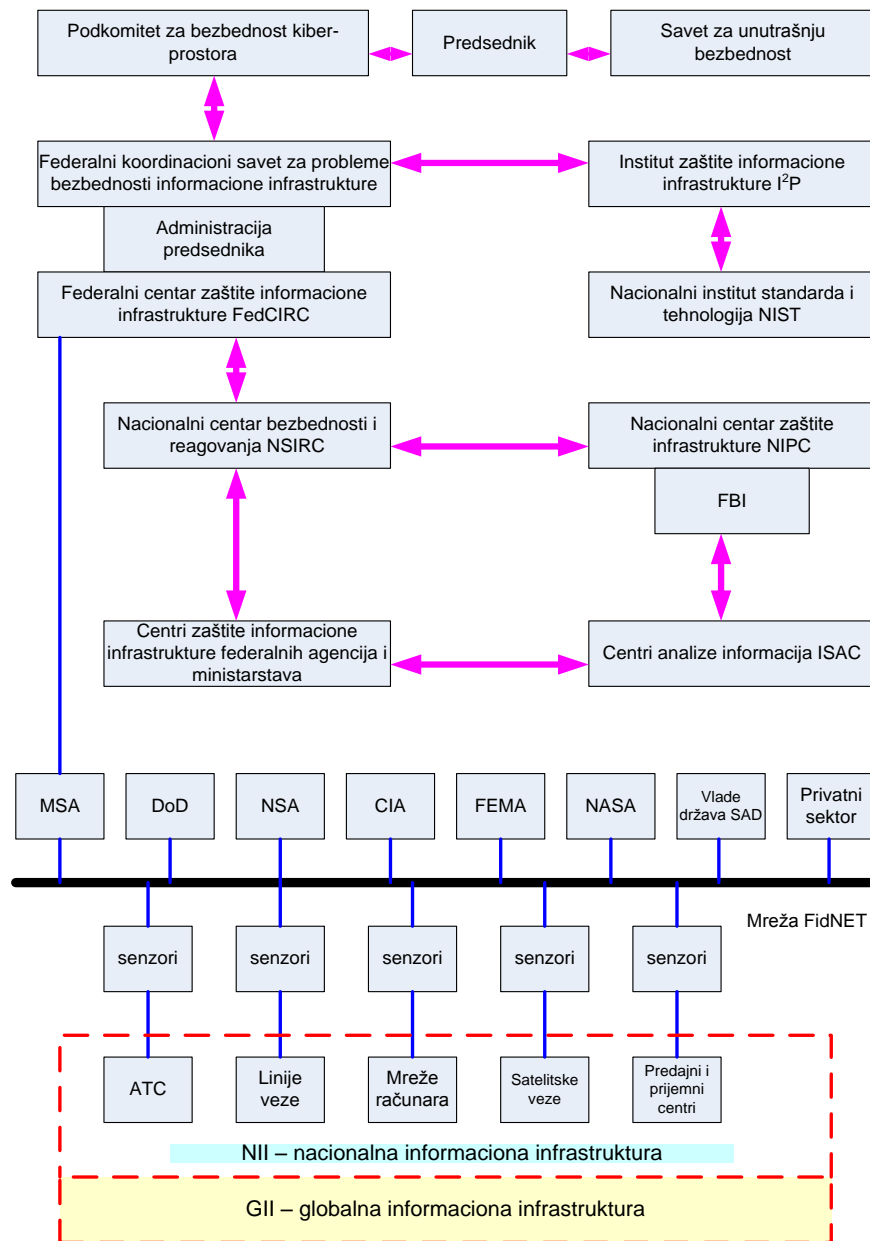


Ekonomski aspekti IB

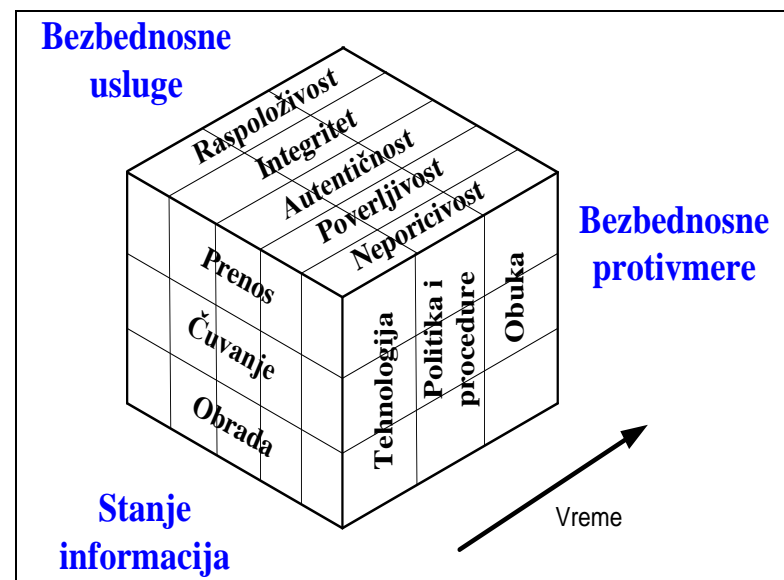
- Posledice neadekvatne zaštite informacija, **oticanja poslovnih informacija firmi** (ekonomska špijunaža, tehnički kanali oticanja informacija i kompjuterski prestupi)
 - koje se ogledaju kao **finansijski gubici, gubitak ugleda ili tržišta** mogu imati katastrofalne posledice.
- Posledice neadekvatne zaštite informacija, u slučaju **državne i vojne tajne**, ponekad nemaju tako jasno i surovo izražene oblike manifestacije gubitaka,
 - ali ne moramo sumnjati da su isto tako, ako ne i više, teške.
- Stručnjaci za informacionu bezbednost tvrde da:
 - Potpuno “otkrivanje” informacionih sistema dovelo bi do **propadanja**
 - **20%** srednjih firmi za nekoliko sati
 - **50%** - za nekoliko dana,
 - Dok bi ostatak “preživeo” nekoliko nedelja
- **Ekonomska cena IB** – princip dovoljnosti – da cena bude manja od mogućih gubitaka

2.3. Nacionalna informaciona infrastruktura





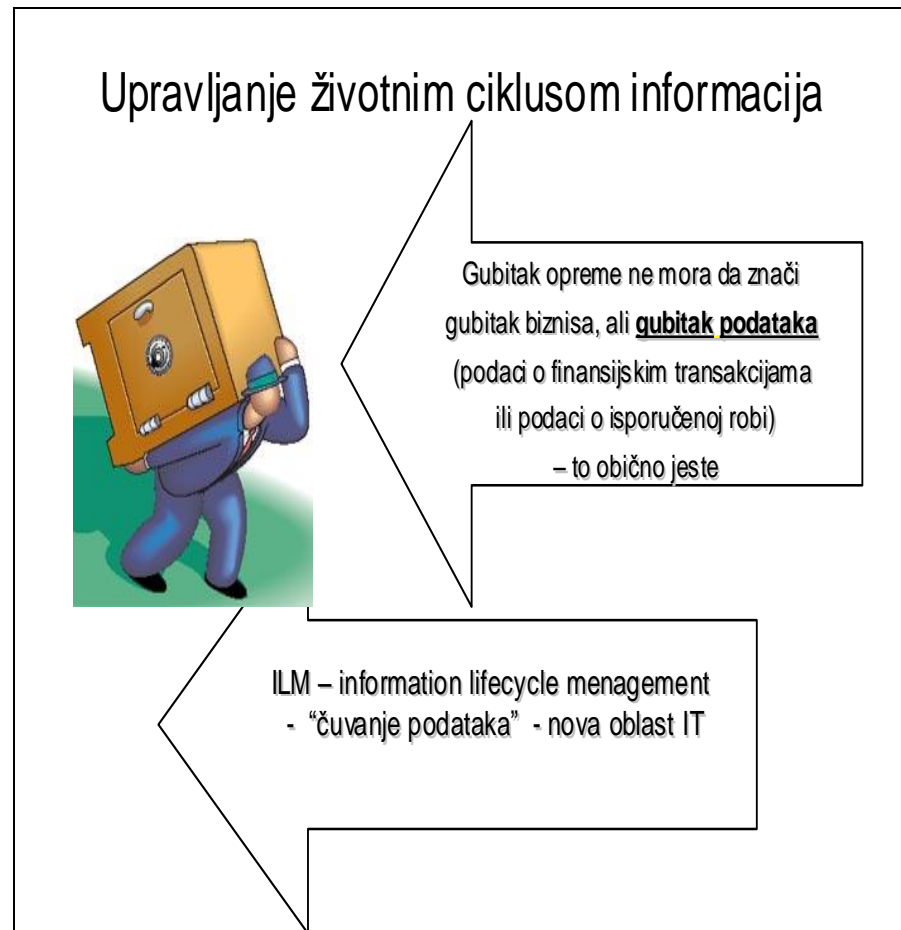
Struktura upravljanja bezbednošću nacionalne informacione infrastrukture SAD



Model information assurance (model IA)

2.4. Informaciona bezbednost u oblasti poslovanja

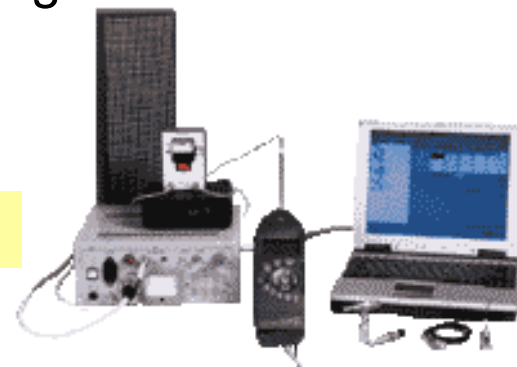
- Obuhvata:
 - **Pribavljanje** informacija
 - Konkurentsko izviđanje
 - Industrijska špijunaža
 - **Upravljanje** životnim ciklusom informacija
 - **Informaciono – analitičko obezbeđenje** poslovanja
 - **Elektronsko poslovanje** i infrastrukturu zaštite i
 - **Cenu** – efikasnost sistema IB



Int-tehnologije i biznis – konkurentsko izviđanje

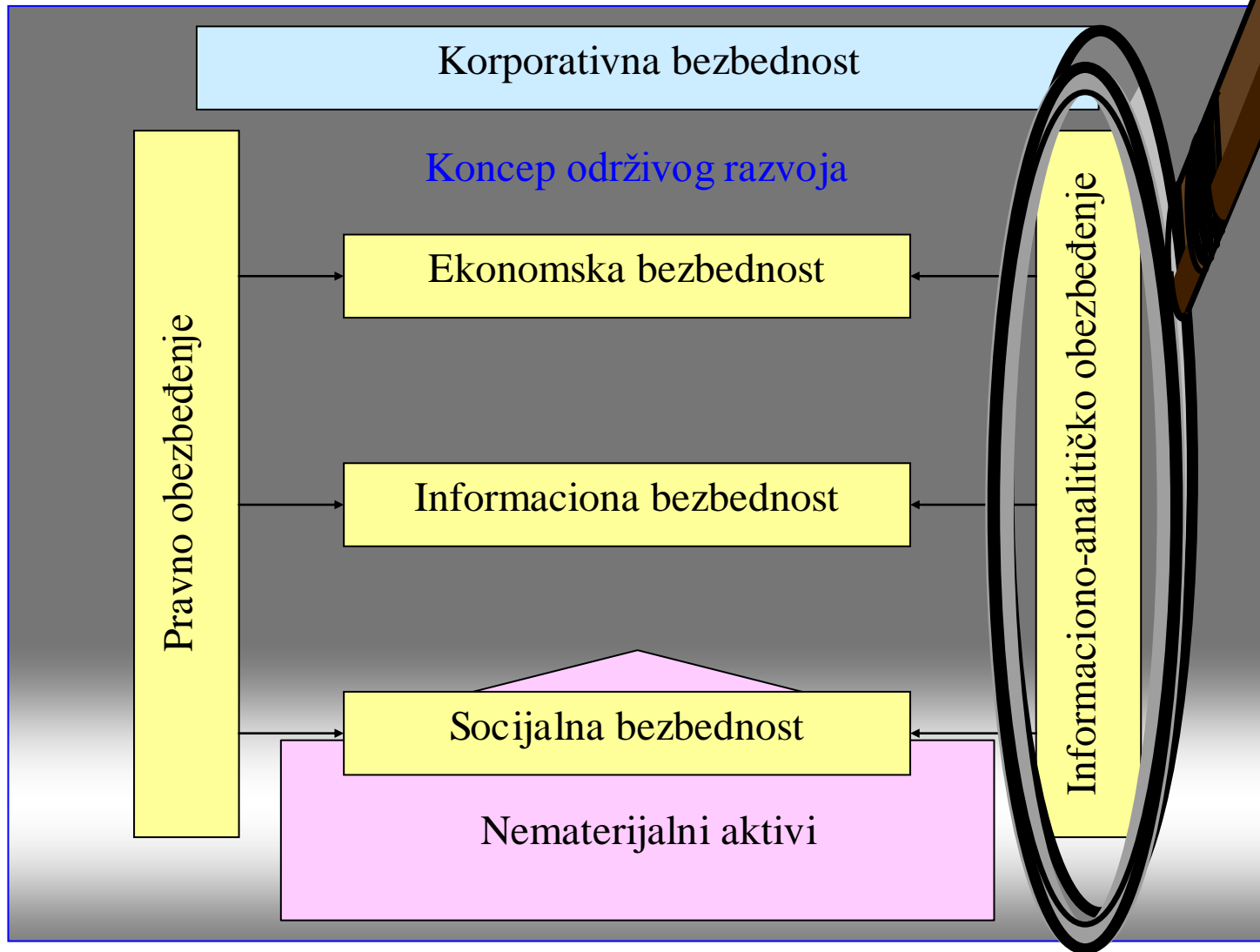
- Konkurencija je savremeni biznis učinala vrlo agresivnim i “žestokim”
- Borba za liderstvo se vodi, praktično, **vojnim metodama** koje dozvoljavaju primenu svih organizacionih i tehnoloških novina
- U toj borbi, kompanije su prinuđene da se oslanjaju na **principijelno nove informacije** (po nakadašnjim shvatanjima – neekonomske).
- Bez takvih informacija, čiji kvalitet je određen blagovremenošću i adekvatnošću, savremene kompanije ne mogu računati na uspeh na globalnom tržištu.

Int-tehnologije



- Postoje dva pravca primene int-tehnologija u obezbeđenju biznisa:
 - Za **povećanje nivoa obaveštenosti o situaciji van kompanije** – u svetu, u zemlji, o stanju aktiva i planova konkurenata, o konjukturi globalnih i regionalnih tržišta i slično.
 - Ovom pravcu pripadaju i mere aktivne korporativne politike koje imaju za cilj povećanje efektivnosti na međunarodnim fondovskim i finansijskim berzama kao i na održanje imidža kreditne sposobnosti kompanije i
 - **Porast nivoa obaveštenosti menadžmenta o situaciji u kompaniji**. Na ovo se odnose i mere aktivne zaštite korporativnih tajni (prevencija insajderskog oticanja informacija).
 - Efektivnost rashoda i sinhroni rad saradnika (rad na podizanju motivacije) se poboljšavaju praćenjem saradnika tzv. mehanizmom int-tehnologija (ugrađen videonadzor svih proizvodnih i radnih procesa)

Informaciono-analitičko obezbeđenje biznisa



4. Zaključak

- Krajnje je vreme da država Srbija, preko svojih organa, **preuzme realizaciju svojih obaveza u sferi IB**
- Osnovni zadatak državnih institucija je **regulisanje korišćenja IS i razmene informacija** u cilju sprečavanja protivpravnih delovanja (preko izrada normativnih dokumenata - doktrina, strategija, zakona, konvencija, saglasnosti i dr., kontrola pravne regulative i regulisanje funkcionisanja pravnih institucija u sferi IB).



- Osnovni zadaci državnih organa u sferi IB povezani su sa **zaštitom opštih interesa**, sprečavanjem protivpravih delovanja, a takođe i sa **zaštitom informacija državnog značaja** (vojni podaci, informacije o specijalnim tehnologijama itd.).
- Pitanja IB u **privatnom sektoru** ekonomije je, po pravilu, prerogativ kompanija i organizacija.
- Za razliku od opštih trendova, u SAD su primetna nastojanja da se **ova dva sektora (privatni i javni) što je moguće više približe i da se jednako tretiraju od strane države** (što je i naša preporuka). Ovo je posledica shvatanja da je bezbednost nedeljiva i nastojanja da se izgradi sveopšta bezbednosna struktura.

STANJE IB U SRBIJI

ČINJENICE:

- *Nemamo Strategiju Informacione bezbednosti*
- *Nemamo Zakon o Informacionoj bezbednosti*
- *Nemamo definisanog osnovnog nosioca posla*
- *Nemamo plan (ako ne računamo preambiciozne Akcione planove koji su svrha sami sebi i lažni dokazi da se nešto radi)*

ČINJENICE:

- *Nemamo planirana sredstva*
- *Nemamo sadejstvo sa svetskom zajednicom iz domena Informacione bezbednosti (CERT)*

ODGOVORNI za stanje u ovoj oblasti **MORAJU** biti svesni da je reč o vrlo **OZBILJNOM** i **SLOŽENOM** **NACIONALNOM** problemu na koji se mora delovati **ADEKVATNO, CELOVITO I HITNO!**

Hvala na pažnji

Mr Zoran Živković, dipl.inž
Kompanija Towers Net
z.zivkovic@towersnet.rs
www.towersnet.rs



TOWERS NET
IT & Telecommunications Innovations

