INFORMACIONA BEZBEDNOST

Stevan Sinkovski,dipl.ing, VP 1100 Beograd
mr Branislav Lučić,dipl.ing, Jugoimport SDPR

Apstrakt: *U ponuđenom radu se razmatra savremeno shvaćen pojam informacione bezbednosti kroz prikaz aktuelnih modela. Ključne reči: informaciona bezbednost, informaciona garancija, zaštita informacija*.

INFORMATION SECURITY

Abstract: *In this paper the terms of information security is examined through the modern review of the relevant models. Key words: information security, information assurance, information protection.*

1. POGLEDI NA POJAM INFORMACIONE BEZBEDNOSTI

Pojam informacione bezbednosti (IB) je nastao u SAD na osnovama teorije informacionog ratovanja (IW - *information warfare*).

Prema rečima Daniela Wolfa[i] [1], istorijski posmatrano, prvo se pojavila 60-ih godina komunikaciona bezbednost (COMSEC – *communication security*). Sa pojavom kompjutera, 70–ih godina, nastala je kompjuterska bezbednost (COMPUSEC – *computer security*). Krajem 80–ih godina COMSEC i COMPUSEC su objedinjene u **informacionu bezbednost** (INFOSEC - *information security*) koja je pokušala da integriše ranije odvojene discipline kao što su bezbednost personala, kompjuterska bezbednost, komunikaciona bezbednost i operativna bezbednost. Akcenat INFOSEC je stavljen na sprečavanje neautorizovanog pristupa informacionim sistemima. Razmatrana je, pre svega, poverljivost (*confidentiality*), integritet (*integrity*) i raspoloživost (*availability*) informacija.

Istorijski posmatrano, 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* [2].

Napredak u kompjuterskoj tehnici i pojava mreža (LAN i WAN i, pre svega, INTERNET'-a), proširuje listu svojstava informacija, pred koje se postavljaju bezbednosti zahtevi. To su: autentičnost (*authentication*) i neporicljivost (*non-repudiation*). Na osnovama navednih svojstava informacija (ili bezbednosnih servisa informacija i informacionih sistema), formulisan je, 90–ih godina, pojam **informacione garancije**[ii] (IA - *information assurance*). Važno je uočiti da razlika nije samo terminološke prirode, već da je reč o suštinskim promenama. Pored navedenih bezbednosnih servisa, informaciona garancija (IA) ima još jednu važnu karakteristiku a to je operativnost (*operational in nature*) i osetljivost na vreme (*time–sensitive*). Ovu karakteristiku izražavaju termini detekcija (*detection*) i reakcija (*reaction*)[iii]. Reč je o defanzivnim operativnim mogućnostima koje se, zajedno sa tradicionalnim IA aktivnostima, od kasnih 90–ih godina opisuju terminom teorije informacionog ratovanja - odbrambenih informacionih operacija (DIO - *defensive information operations*)[iv] [1,3].

Konačno 2002.godine direktivom MO SAD (DoDD Namber 8500.1 *Information assurance*, octobar 24, 2002) zvanično je uveden pojam informacina garancija. 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»*[v].

Kada je reč o informacionoj bezbednosti, u SAD, postoji tesna saradnja državnog i privatnog sektora što je definisano i u svim doktrinarnim dokumentima.

Evropske zemlje, u svom shvatanju pojma informacione bezbednosti, sa naglašenijim pragmatičnim pristupom[vi], prate poglede SAD [4].

Razmatranje pojma informacione bezbednosti (*информационная безопасность*) u Ruskoj federaciji je novijeg datuma (od 90-ih godina). Prema nekim autorima [5] bivši SSSR je izgubio hladni rat zbog zanemarivanja bezbednosti u informacionoj sferi društva.

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)* [6] odnosno kao **stanje zaštićenosti informacione sredine** *društva koje omogućava njeno formiranje, korišćenje i razvoj u*

interesu građana, organizacija, države[vii]. Kao polazno stanovište pri definisanju pojma uzet je interdisciplinarni pristup - opšta nauka o bezbednosti.

Uočavamo da se u «*Doktrini informacione bezbednosti Ruske federacije*» termin informaciona bezbednost koristi u širem smislu, dok je u zapadnim shvatanjima reč o užem smislu pojma jer se odnosi samo na informacije i informacione sisteme (IS).

U okviru tzv. «ruske škole» razlikujemo nekoliko pravaca: predstavnike humanitarnih nauka koji ostaju na nivou opštosti (konceptualni modeli IB), predstavnike bliske zapadnim gledištima i predstavnike koji pojmu zaštita informacija (pojam blizak slovenskim jezicima) daju nova obogaćena značenja, ne samo njegovim proširivanjem npr. *integralna zaštita informacija*, već i sadržajno.

Po nekim autorima, informaciona bezbednost je **disciplina** informacione tehnologije jer je ona njena osnovna komponenta.

U Republici Srbiji problematika informacione bezbednosti nije, kao takva, dovoljno razmatrana. Pod terminima *zaštita informacija*, *bezbednost i zaštita informacija* ili *zaštita podataka* tretirani su neki od aspekata informacione bezbednosti. Činjenica da je, prema savremenim shvatanjima pojma nacionalne bezbednosti, informaciona bezbednost jedna od njenih osnovnih komponenti, problematiku informacione bezbednosti čini krajnje aktuelnom [7].

2. MODELI INFORMACIONE BEZBEDNOSTI

Modeli informacione bezbednosti su aproksimativni okviri koji, na očigledan način, kvalitativno i kvantitativno predstavljaju problematiku informacione bezbednosti. U tekstu koji sledi upoznaćemo se sa nekim od aktuelnih modela informacione bezbednosti kao i nekim softverskim paketima iz ove oblasti.

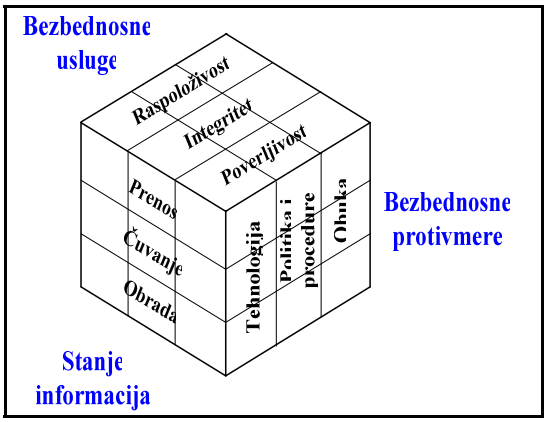
2.1. Kvalitativni modeli informacione bezbednosti

Integralni model informacione bezbednosti

Integralni model informacione bezbednosti (McCumber INFOSEC model, slika 1) je prvi put publikovan 1991.godine. Reč je o modelu zasnovanom na integralnom prilazu svim aspekata informacione bezbednosti [8]. U skladu, sa tada važećom definicijom informacione bezbednosti, definisane 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*, model informacione bezbednosti tretira tri aspekta:

1. ***stanje*** u kojima se nalaze informacije (prenos, čuvanje i obrada),
2. ***bezbednosne usluge*** (raspoloživost, integritet i poverljivost) i
3. ***bezbednosne protivmere*** (u oblasti tehnologija, politika i procedura kao i obuke)

Ovako definisan model je trodimenzionalan.



Sl 1: Originalni McCumber model [8]

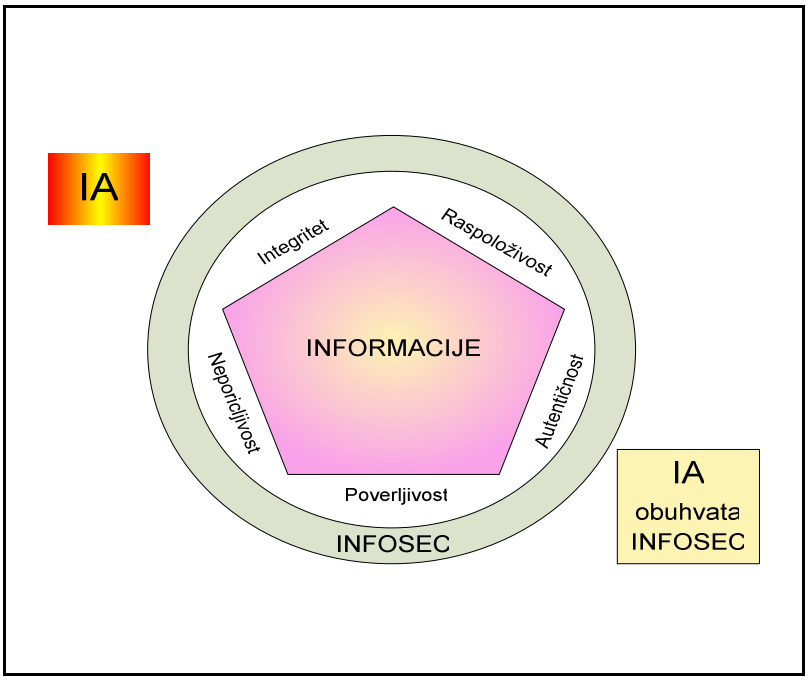
Na osnovu ovog modela napisan je kanadski kriterijum za procenu informacione bezbednosti CTCPEC[viii] [8].

Model informacione garancije

Model informacione garanacije (IA) predstavlja novi, multidisciplinarni i multidimenzionalni pogled na važne elemente McCumber-ov modela.
Informaciona garancija je (prema NSTISSC, zajedničkoj doktrini informacionih operacija JP 3-13, 1998:1-9 i u pravilu KoV-a FM 3-13, 2003. god..) 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».*

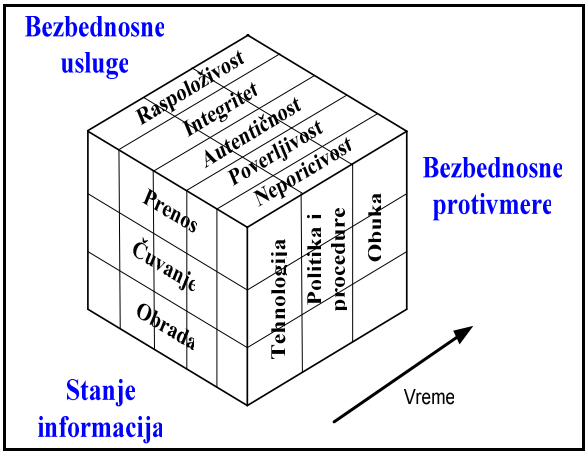
Za razliku od informacione bezbednosti, informaciona garancija je definisana kao **informacione operacije** sa skupom svih odbrambenih i proaktivnih komponeti što njihovu razliku čini suštinskom, a ne samo semantičkom. Informaciona garancija obuhvata ulogu informacione bezbednosti (slika 2, [8]).

Informaciona garancija je proširila listu bezbednosnih zahteva (poverljivost, raspoloživost i integritet) i na svojstva informacija kao što su autentičnost (*authentication*) i neporicljivost (*non-repudiation*). Pored navedenih bezbednosnih servisa, informacionu garanciju (IA) karakterišu operativnost (*operational in nature*) i osetljivost na vreme (*time–sensitive*).



Sl. 2: Odnos između informacione bezbednosti i informacione garancije IA

Model IA je četvorodimenzionalan i obuhvata: **stanje** informacija, **bezbednosne servise** (usluge), **bezbednosne protivmere** i **vreme** (slika 3). Pomoću ovakvog modela mogu su predstaviti svi odbrambeni elementi odbrambenih informacionih operacija (DIO).



Sl. 3: Model informacione garancije (model IA)

Za razliku od konvencionalnog modela, on obuhvata i mere zaštite sistema (detekcija, reakcija) kao i rezidentne informacije u takvom sistemu (restauracija). Sinonim ovih osobina informacionih sistema je sposobnost preživljavanja (*survivability*). Otpornost na napade («žilavost») informacionih sistema se u literaturi razmatrala i ranije kao sposobnost opstanka, preživljavanja Sposobnost preživljavanja je definisana kao «**sposobnost** *sistema da izvršava misije na pogodan način uprkos napadima, otkazima ili nepredviđenim događajima*» [9]. Ključna osobina sposobnosti preživljavanja mrežnih sistema[ix] je njihova sposobnost da održe osnovne servise (određene nivoe integriteta, poverljivosti, performansi i drugih kvalitativnih svojstava) tokom napada i u vreme pada sistema ili nesreće.

Ešelonirani model informacione bezbednosti

Sa svakim novim dostignućem u oblasti informacionih tehnologija (npr. «virtuelna organizacija» [x]) javljaju se novi aspekti informacione bezbednosti. Jedan od primera «virtuelnih organizacija» je **Globalna informaciona mreža** (GIG – *global information grid*) nastala za potrebe Pentagona koja treba da omogući upravljanje mobilnim i kompaktnim borbenim sastavima.
Klasični modeli IB zasnovani na autonomnosti i lokalnosti resursa IS, ne zadovoljavaju savremene network-centric zahteve. Rešenje je ešelonirani, višeslojni model IB[xi]. Koncept ešeloniranog modela obuhvata skup komponenata koje realizuju funkcije monitoringa, zaštite i adaptacije informacionih resursa.

Kako savremena teorija i praksa informacione bezbednosti zahteva racionalan pristup, koji omogućava efikasno korišćenje svih raspoloživih resursa (ljudski, finansijski i materijalni), to ečelonirani model mora zadovoljti i uslove **adaptivnog upravljanja bezbednošću** (*adaptive network security*)[xii] zasnovanog na **koncepta upravljanja rizikom** .



Sl. 4: Ešelonirani model informacione bezbednosti

Model adaptivnog upravljanja bezbednošću ugrađen je u standard ISO/IEC 15408. Prema njemu, za zaštitu informacione infrastrukture u SAD, primenjuje se **model ešelonirane višeslojne informacione bezbednosti** (slika 4) [xiii] koji realizuje funkcije monitoringa, zaštite i adaptacije informacionih resursa. Na taj način moguće je sprečavanje prodora, detekcija narušavanja bezbednosti, lokalizacija napadnutog objekta, neutralizacija, eliminisanje napadača i rekonstrukcija izgubljenih funkcija sistema. U osnovi datog modela leži primena pasivnih (filtera, međumrežnih ekrana - *firewal*) i aktivnih (senzora detekcije napada, raspoznavanja anomalija, adaptivnih algoritama rekonstrukcije) tehničkih sredstava zaštite. Najpoznatija od savremenih tehnologija ove namene je tehnologiji IDS (*Intrusion detection Systems* – detekcija napada na sistem) [10].
Suština modela informacione bezbednosti je povećanje zahteva u pogledu «preživljivosti» (*survivability*) informacionih sistema, a posebno onih koje karakteriše visok stepen raspodeljenosti resursa i, praktično, potpuno odsustvo centralizovanog upravljanja.

Model zaštitnih prstenova

Model ešelonirane višeslojne informacione bezbednosti svoju detaljnu, preglednu i lako shvatljivu razradu, na nivou pojedinačnog informacionog sistema, dobio je u **modelu zaštitnih prstenova** [11,12] koji, IB IS, razmatra sa više aspekata: pravne norme, organizacione mere, mere neposredne zaštite, zaštita opreme, zaštita programske podrške i zaštita baza podataka.

Zaštitni prstenovi su: **humani prsten** (personal koji radi sa svojim motivima, spremnošću i mogućnošću delovanja), **normativni prsten** (obavezuje i propisuje izvršenje i način izvršenja neke radnje, definisan matricom ovlašćenja), **organizacioni prsten** (mere i aktivnosti, nadležnosti i obaveze korisnika i izvršilaca), **prsten fizičke zaštite** (onemogućava fizički pristup napadača), **zaštita softvera** (kontrolisano čuvanje i kopiranje operativnog sistema i aplikativnih programa), **zaštita (rezidentnih) podataka** (obuhvata ograničenje pristupa podacima, evidentiranje pristupa podacima i sprečava neovlašćeni pristup podacima), **zaštita infrastrukture** (obezbeđuje optimalne uslove za funkcionisanje svih komponenti IS), **protivpožarna zaštita** (građevinske mere, primena odgovarajućih sredstava za gašenje i obuku osoblja), **zaštita IS u radu u mrežnom okruženju** (kontrola pristupa mreži i kriptozaštita poruka koje se prenose u difuznoj računarskoj mreži) i **kriptozaštitni bezbednosni prsten** (kriptozaštita podataka tranzicijom ili supstitucijom).
U modelu zaštitnih prstenova uočavamo, na nivou pojedinačnog informacionog sistema, ešeloniranu po dubini zaštitu informacija. Model pokriva široku lepezu mogućih napada što je karakteristično za uslove savremenog življenja. U njemu se vide i elementi integrisanih sistema.
Na višem nivou uopštavanja zaštitne prstenove možemo definisati kao: legalnu i društvenu kontrolu (pravni okvir), administrativnu kontrolu (organizacione mere), fizičku zaštitu i kontrolne procedure u sistemu.

Model sa objektno-orijentisanim prilazom informacionoj bezbednosti

Prema shvatanju V. Galatenka[xiv] informaciona bezbednost je **zaštićenost** informacija i podržavajuće infrastrukture[xv] od slučajnih ili namernih dejstava prirodnog ili veštačkog karaktera koja mogu naneti **neprihvatljive gubitke subjektima informacionih odnosa** pa, u tom smislu, i vlasniku i korisniku informacija kao i podržavajućoj infrastrukturi.

Definicija uvodi kategorije *informacionih odnosa* (između različitih subjekata sa različitim interesima) i *neprihvatljivih gubitaka* (apsolutna zaštita ne postoji zbog čega se uvodi upravljanje rizicima koje podrazumeva uvođenje praga prihvatljivosti gubitaka – obično materijalno izraženi).

Polazeći od činjenice da su informacioni sistemi uglavnom bazirani na kompjuterima i tehnikama programiranja, V. Galatenko smatra da je u tretiranju IB, umesto strukturnog prilaza, potrebno koristiti najsavremenije tehnologije programiranja – objektno-orijentisano (OO) programiranje.

Savremeni informacioni sistemi predstavljaju distribuirani skup uzajamno delujućih objekata[xvi]. Svaki objekat pruža drugom objektu neke usluge (servise). U ovako tretiranom pojmu IS, informaciona bezbednost je obezbeđena sledećim servisima: identifikacija/autentifikacija, razgraničenje pristupa, protokoliranje/audit, ekraniranje, tuneliranje, enkripcija, kontrola integriteta, kontrola zaštićenosti, detekcija i neutralizacija otkaza, operativna restauracija i upravljanje.

Objektna dekompozicija (ponašanje sistema se opisuje u terminima uzajamnog delovanja objekata) i principi OO programiranja (detaljizacija, nasleđivanje, polimorfizam i inkapsulacija) omogućavaju da se cilj IB (svojstva informacija: raspoloživost, integritet i poverljivost) i sredstva za njegovo postizanje (zakonodavne mere, administrativne mere, proceduralne mere i programsko-tehničke mere) predstave tzv. granama (nitima) OO programiranja (relativno nezavisne karakteristike objekata).

Servise bezbednosti se objedinjavaju, u cilju dizajniranja **ešelonirane odbrane**, metodama OO programiranja – pomoću aktivnih agenata. Na svojstvima objekata, kontejnera i unikalnih identifikatora, formiraju se funkcionalni paketi, bazni i izvedeni profili zaštite u skladu sa standardima u oblasti informacione bezbednosti.

Rezimirajmo, informaciona bezbednost je zaštita interesa subjekata informacionih odnosa. Uspešna IB podrazumeva kompleksan prilaz koga čine mere na četiri osnovna nivoa: **zakonodavnom, administrativnom, proceduralnom i programsko-tehničkom** [13].

Konceptualni model informacione bezbednosti

Shvatanje pojma informacione bezbednosti u širem smislu prisutno je u konceptualnom modelu istraživača iz domena društvenih nauka (A.D.Ursul i T.N. Cirdja[xvii]).

Konceptualni model informacione bezbednost je zasnovan na sledećim postavkama. Informaciona bezbednost je bezbednost u informacionoj sferi - **infosferi**. Fizički infosfera se sastoji od tri elementa: informacione infrastrukture (uređaji za prenos i obradu informacija), informacija i njihovih tokova i personala koji obavlja različite delatnosti. Informaciona sfera je nastala kao posledica nastanka nove društveno-ekonomske formacije društva – informacionog društva. Nova društveno-ekonomska formacija društva povlači za sobom i nove suprotnosti i nove pretnje (opasnosti). Nove pretnje iziskuju nove pristupe. U domenu informacione sfere, s jedne strane, potrebno je obezbediti društvo informacionim resursima a, sa druge strane, formirati sistem zaštite informacionih potencijala. Imperativ informacionog društva je informaciona dominacija u životno važnim oblastima. **Osnovni sukob informacionog društva je je sukob u mogućnosti pristupa informacijama** [14].

Ako je bezbednost odsustvo pretnji ili mogućnost pouzdane zaštite od njih [15], onda je «informaciona bezbednost odsustvo informacionih pretnji, ili stanje zaštićenosti, i stabilnost osnovnih sfera ljudskih delatnosti u odnosu na moguća informaciona dejstva». U tom kontekstu informaciona bezbednost je svojstvo socijalnog sistema pozvana da garantuje takvo stanje informacionih pojava koje obezbeđuju čoveku i društvu u celini informacione uslove preživljavanja i daljeg stabilnog razvoja. Informaciona bezbednost se rasprostire na sve pojave infosociosfere čiji elementi, direktno ili indirektno, «rade» na optimalnoj evoluciji društvenog sistema obezbeđujući uslove za bezbedan razvoj a samim tim i progres.

Na taj način «informaciona bezbednost je **sposobnost** države, društva, socijalnih grupa i ličnosti:

1. *da obezbede sa određenom verovatnoćom dovoljne i zaštićene informacione resurse i socijalni intelekt, optimalnu socijalnu entropiju i infosferu za podršku životnih delatnosti i životnih sposobnosti, stabilnog funkcionisanja i razvoja sociuma,*
2. *da se suprotstave informacionim pretnjama i napadima, negativnim informacionim delovanjima na individualno i društveno znanje i psihu ljudi kao i na računarske mreže i druge tehničke izvore informacija,*
3. *da formiraju lične i grupne navike umeća bezbednog ponašanja,*
4. *da podrže konstantnu raspoloživost u odnosu na adekvatne mere informacione protivodbrane,*
5. *da konstantno i, po određenom programu bezbednosti, iterativno inkorporiranje veštačku inteligenciju u socisredinu.*

U takvoj interpretaciji, **informaciona bezbednost se javlja ne samo kao jedan od oblika bezbednosti, već i kao presek svih tih oblika u sferi delovanja u kojima informacione tehnologije zauzimaju važno mesto**» [15].

Sistemski prilaz obezbeđenja informacione bezbednosti u infosferi obuhvata tri celine:

1. *humanitarnu* povezanu sa razvojem duhovne sfere društva i pravima građana u oblasti informacionih delatnosti (formiranje i korišćenje informacionih resursa),
2. oblast *informatizacije* (formiranje i razvoj jedinstvenog informacionog prostora regiona, zemlje i svetskog informacionog polja) i

3. oblast obezbeđenja bezbednosti funkcionisanja *informacione infrastrukture* [14].

Sistemski prilaz u objašnjenju suštine i sadržaja pojma informacione bezbednosti predstavljen je u **konceptualnom modelu** (tablica 1).

Informacija	
Izvori informacija	ljudi, dokumenta, publikacije, sredstva masovnih informacija, tehnički nosioci (medijumi), tehnička sredstva, proizvodnja, proizvodni otpadci
Pretnje (opasnosti)	integritetu, poverljivosti, potpunosti, pouzdanosti pristupa
Izvori napada	protivnici, konkurenti, prestupnici, korupcioneri, strukture vlasti
Ciljevi	upoznavanje, modifikacija, uništavanje
Objekti napada	podaci o sastavu, stanju i delatnostima
Načini pristupa	na račun razglašavanja, na račun oticanja, na račun neovlašćenog pristupa
Pravci zaštite	pravni, organizacioni, tehnički
Sredstva zaštite	fizička, hardverska, softverska, kriptografska
Metode zaštite	predupređenje, odvraćanje, presecanje, protivdejstva

Tabela 1: Konceptualni model informacione bezbednosti [14]

Informaciona bezbednost se može posmatrati i u kontekstu koncepta «*uzajamne povezanosti*» kao dominirajućeg koncepta bezbednosti informacionog društva [15]. Suština koncepta je prelazak od informacionog ratovanja ka upravljivim sukobima i partnerstvu (*управляемая конфронтация и сотрудничество*).

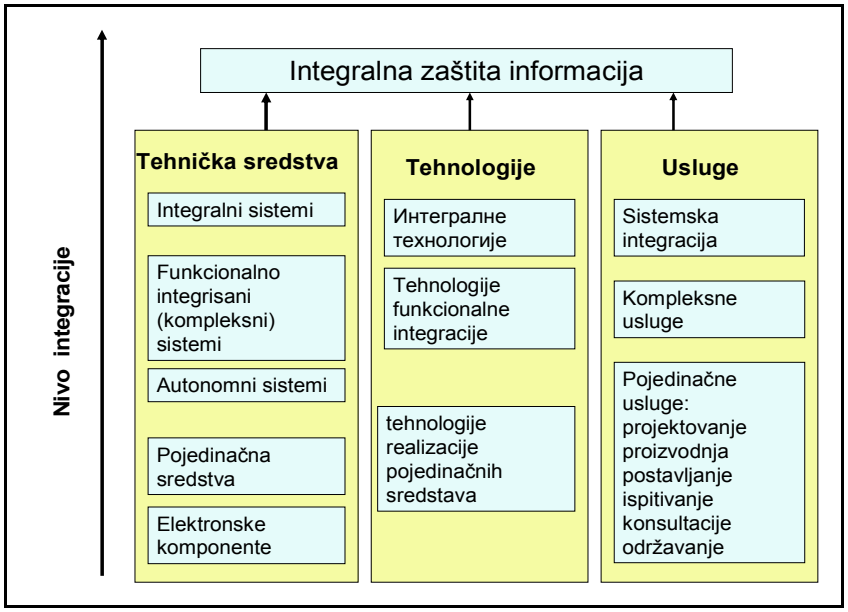
Informacino ratovanje, kao poseban oblik informacionog suparništva ne ograničava se samo na dezorganizaciju i blokiranje mehanizama upravljačkih struktura. Zbog prirode informacionog prostora, informaciona dejstva nose u sebi ne samo logički (podčinjavanje), već i sociotehnički (upravljački) karakter. Različiti odnosi logičkog u sociotehničkog u informaciji, menjaju karakter informacione protivodbrane: od rata (koji se vodi za postizanje ranije postavljenih ciljeva) do informacione igre. Pobeda u informacionoj igri je mogućnost da se dođe do odluke.

Za prelazak od informacionog ratovanja ka upravljivom sukobu i partnerstvu potrebno je da informacije budu svima dostupne (da budu «otvorene») jer se na taj način povećava stepen višeznačnosti i mogućnost predikcije (prognoze) informacija na račun informacione igre. Paradoks situacije je činjenica da dostupnost informacija podrazumeva saglasnost i međusobno poverenje među društvenim i političkim snagama koje, bez dostupnosti informacija, nije moguće. Jedno od rešenja je pomeranje težišta sa protivodbrane na prikupljanje i analitičku obradu informacija kao sredstva predviđanja oblasti sistemskih sukoba. Kao rešenje se javlja i inteziviranje informaciono-komunikativnih dejstava među subjektima.

Model integralne zaštite informacija

Model integralne zaštite informacija (*интегрална защита информации*) je zasnovan na konceptu **integralne bezbednosti** (D.V.Barsukov).

Osnovni smisao pojma integralne bezbednosti se sastoji u *neobhodnosti obezbeđenja takvog stanja uslova funkcionisanja* **čoveka, objekata** i **informacija** u kom su oni pouzdano zaštićeni od svih realnih vidova pretnji u toku neprekidnog proizvodnog procesa i svih životnih delatnosti [16]. Naime, u svakodnevnom životu ljudi se susreću sa različitim vrstama bezbednosti: od požara, ličnoj, finansijskoj, ekološkoj itd. Naravno, ovakva podela je uslovna. *Ako posmatramo informacije, jasno je da je njihova efikasna zaštita moguća samo u tom slučaju ako je bezbednost, od svih vrsti pretnji, garantovana ne samo podacima, već i uređajima u kojima se oni obrađuju i čuvaju, kao i licima*[xviii] *koji rade sa tim podacima* [16].



Sl. 5: Integralna zaštita informacija [16]

Konačan **cilj** *integralne zaštite informacija je stvaranje takvih uslova pri kojima je nemoguće presretanje, falsifikovanje i uništavanje informacija. Dejstvo ovakve zaštite mora biti neprekidno u vremenu i prostoru* [16].

Jedan od osnovnih zahteva savremene zaštite informacija je **sistemski prilaz**. **Integralni prilaz** informacionoj bezbednosti podrazumeva otklanjanje svih mogućih opasnosti uključujući i sve kanale oticanja informacija (njihovo blokiranje) koristeći se savremenim naučnim dostignućima i integracionom tehnologijama (slika 5). Realizacija takvog prilaza zahteva objedinjavanje različitih podsistema bezbednosti u jedinstven sistem koji sadrži tehnička sredstva (osnovna i pomoćna), kanale za komunikaciju, programsku podršku, baze podataka i obučen personal.

Prednost navedenog modela je činjenica da pored kompjuterske bezbednosti obuhvata i zaštitu govornih i video informacija, što je aktuelno u kontekstu industrijske špijunaže i poslovnog izviđanja. Nedostatak je što previše insistira na tehničkim aspektima zaštite informacija ne potencirajući dovoljno pravne, organizacione, sociološke i psihološke aspekte.

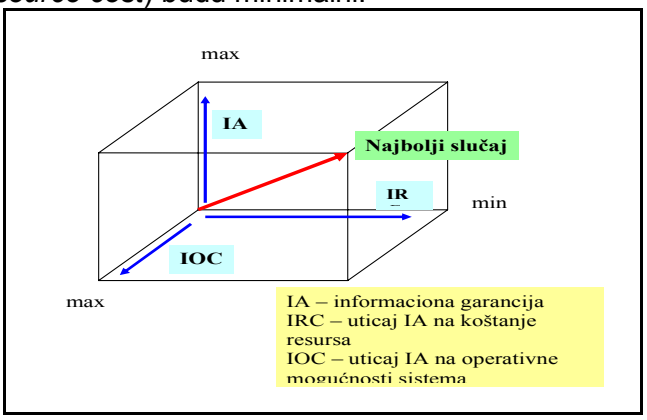
2.2. Kvantitativni modeli informacione bezbednosti

Kvantitativni model Džozefa Bogarda

Kvantitativni model Džozefa Bogarda (Josef Beauregard) je zasnovan na metodologiji fokusiranog vredonosnog mišljenja (VFT – *value focused thinking*)[xix] i modelu IAAM (*information assurance anylisis model*)[xx].

Model IAAM omogućava trodimenzionalno razmatranje problema informacione garancije (slika 6). Svaka od dimenzija (informaciona garancija IA, uticaj IA na operativne mogućnosti sistema IOC, uticaj IA na koštanje resursa IRC) predstavljena je vredonosnom hijerarhijom. Elementi vredonosnih hijerarhija imaju svoje kvantitativne mere. Preračunavanja, za konkretne strategije IA, vredonosnih hijerarhija i njihovih kvantitativnih veličina vrše se pomoću posebno prijektovanog informacionog sistema AMIS (*AFTC Mission information system*) [17].

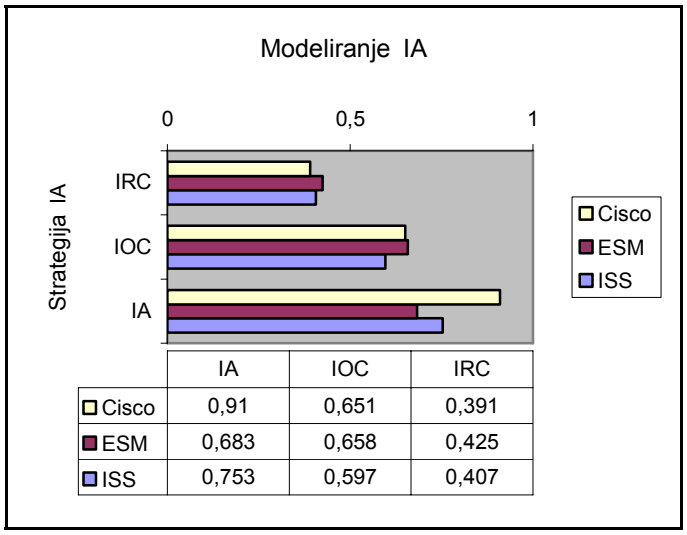
Najbolja strategija IA nastoji da poveća informacionu garanciju IA i operativne mogućnosti sistema IOC (*IA on system operational capability*), a da, pri tome, troškovi resursa IRC (*IA on resource cost*) budu minimalni.



Sl 6: Relacije između IA, IOC i IRC [17]

U model IAAM je implementirana strategija IA jer on obuhvata sva tri faktora koji, svaki za sebe, imaju svoje vredonosne hijerarhijske skale.

Informaciona garancija je proces koji uključuje sposobnost zaštite informacija i informacionih sistema, detekciju događaja koji mogu interferirati sa informacijama i IS i osobinu reakcije u nastaloj neželjenoj situaciji podrazumevajući i sposobnost restauracije osnovnih funkcija sistema. Ovako definisana IA nije sinonim za kompjutersku bezbednost. Reč je o mnogo širem, robusnom konceptu koji obuhvata celokupan proces zaštite informacija, informacionog sistema i informacionog procesa.



	IA	IOC	IRC
Cisco	0,91	0,651	0,391
ESM	0,683	0,658	0,425
ISS	0,753	0,597	0,407

Sl. 7: Rezultat modeliranja IA (preuzeto iz [17])

Zaštita informacija i IS definiše postojanje mera zaštite od neautorizovanih promena. Pored obezbeđenja raspoloživosti, integriteta i poverljivosti, model uvodi meru smanjenja poznatih ranjivih mesta (*compliance*).

Detekcija se definiše kao sposobnost sistema ili personala da detektuju nepoželjne događaje (napade). Detekcija ima tri vredonosne podkategorije blagovremenost, odgovornost i fleksibilnost sa svojim elementima.

Reakcija se definiše kao sposobnost reagovanja na identifikovani napad, sposobnost restauracije informacija i IS i mogućnost učenja i adaptacije na osnovu prethodnih događaja [17].

Promene u informacionoj garanciji IA utiču na operativne mogućnosti sistema IOC. Osnovne podkategorije IOC su efikasnost, funkcionalnost, pogodnost, komfornost za rad i flesibilnost za usavršavanje i proširivanje. Sa slike vidimo da su obuhvaćene gotovo sve značajne osobine sistema (kapacitet, mogućnost prelaska na nove misije, raspoloživost, kompatibilnost, pristupačnost, kompleksnost za upotrebu, vreme ugradnje, testiranje ispravnosti i upotreba prethodne istorije) [17].

Uticaj informaciong obezbeđenja IA na cenu resursa IRC preko podkategorija kao što su cena životnogi ciklusa sredstava i personal. Personal se razmatra kao «korisnik» sa potrebnim psihofizičkim i obrazovnim karakteristikama i kao «podrška personala» koja obuhvata potrebno vreme obuke, treninga i brojčano stanje. Ovim faktorom obuhvaćena je logistička podrška.

Pri izboru strategije IA vrši se proračun za tri slučaja: najbolji, verovatni i najgori. Kao referentna veličina služi osnovni (bazni) sistem. Rešenje kvaliteta strategije IA (sistema) se dobija u vidu normiranog broja na osnovu čega se vrši klasifikacija. Pored ukupnog rešenja, moguće su analize osetljivosti pojedinih vredonosnih kategorija.

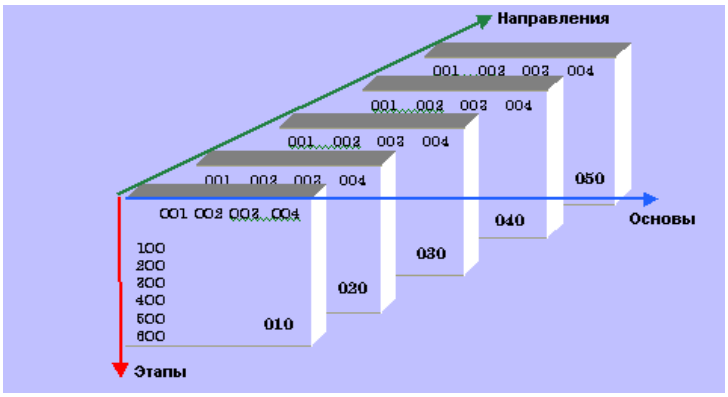
U svojstvu primera i ilustracije predloženog metoda modeliranja IA, preuzet je jedan od mnogobrojnih rezultata iz [17]. Dijagram na slici 7 pokazuje kvantitativne rezultate modeliranja na osnovu kojih je moguće izvršiti izbor strategije IA.

Kvantitativni model sistema zaštite informacija

Sistemski prilaz modeliranju procesa projektovanja i ocene efektivnosti sistema zaštite informacija (SZI) predložio je V. Domarev [18].

Model SZI je zasnovan na modelu sistema IB koga čine: analiza prilaza i koncepcija projektovanja SZI (osnovne komponente), analiza strukture IS (oblasti ZI) i ana-

liza metoda projektovanja SZI (metodološki koraci), slika 8. Na osnovu njihovih komponenata formira se «matrica znanja» kuju čini 4 x 5 x 7 = 140 elemenata.



Slika 8: Merne koordinate – tri grupe komponenti modela SZI

«Matrica znanja» je trodimenzionalna (sl. 9), ali se može predstaviti u vidu Rubikove kocke (sl. 10) - radi upoređenja sa modelom IB i IA - ili u vidu tri dvodimenzionalne matrice, koje uspostavljaju vezu između različitih elemenata matrice.

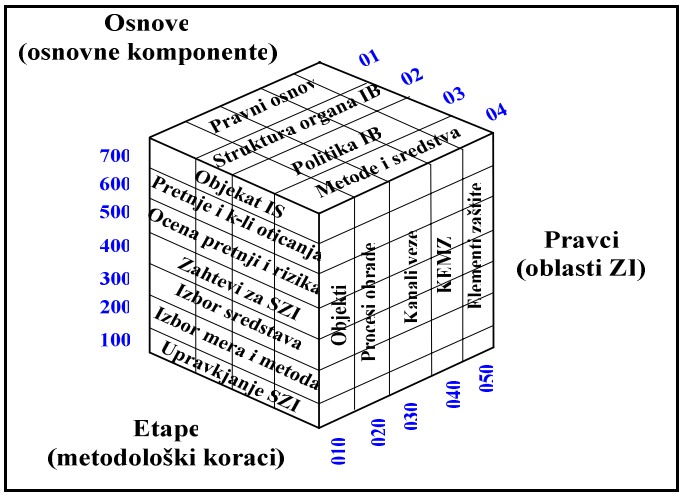
<<< Этапы		010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите																				
200	Выявление угроз и каналов утечки информации																				
300	Проведение оценки уязвимости и рисков																				
400	Определение требований к СЗИ																				
500	Осуществление выбора средств защиты																				
600	Внедрение и использование выбранных мер и средств																				
700	Контроль целостности и управление защитой																				

Sl. 9: Primer numeracije elementa "matrice znanja" No 321

Komponente modela su:

- **koordinata «osnove»**: zakonodavna, normativno-metodološka i naučna osnova, struktura organa koji realizuju zaštitu, politika IB (organizaciono-tehničke mere) i metode, načini i sredstva zaštite informacija
- **koordinata «pravci»**: zaštita objekata IS, zaštita procesa, procedura i programa obrade podataka, zaštita kanala veze, sprečavanje KEMZ-a i upravljanje sistemom zaštite
- **koordinata «etape»**: definisanje objekata IS, detekcija pretnji i kanala oticanja informacija, procena pretnji i kanala oticanja informacija, definisanje zahteva koji se postavljaju pred SZI, izbor sredstava zaštite, izbor mera, načina i sredstava zaštite i upravljanje zaštitom informacija.

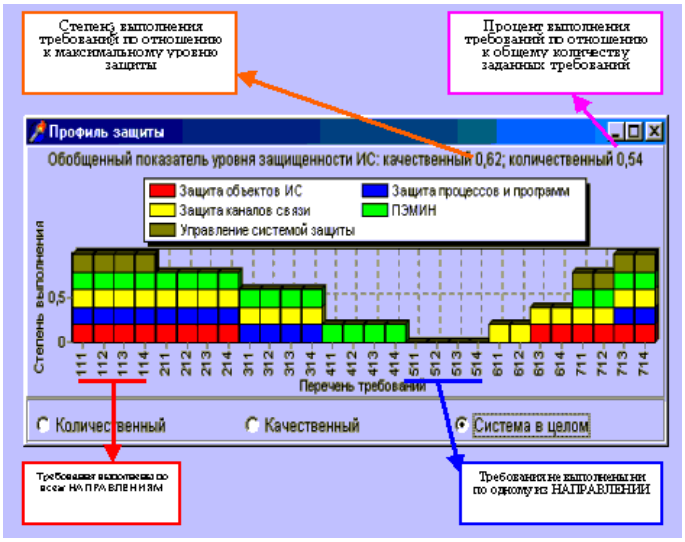
Dvodimenzionalne matrice je moguće primeniti: kao uputstvo za projektovanje SZI, kao dovoljno tačan katalog tehničkih zahteva i kao sredstvo ocene efektivnosti SZI (po 140 pokazatelja).



Sl. 10: Model SZI u formi Rubikove kocke

U modelu SZI, u skladu sa zahtevom da se uspostave ***logičke veze*** između elemenata matrice i zbog neodređenosti ponašanja i krajnjih ciljeva SZI (nejednoznačnost rešenja adaptivnih sistema podložnih korekciji), kao matematički aparat upotrebljena je teorija «nejasnih (нечетких) skupova» u cilju optimizacije [18].

Kao ilustracija modela SZI, na slici 11, prikazana je ocena efektivnosti (poklapanja zadatih zahteva i realizovane zaštite) SZI.



Slika 11:Grafička predstava ocene efektivnosti SZI

Model SZI daje i kvalitativne i kvantitativne ocene na osnovu kojih se formira i uopštena ocena sistema SZI. Sam model je, inače dat u programskoj formi, intrigantan. Ono što je uočljivo na prvi pogled to je da je ekonomski aspekt, u smislu cene koštanja projektovanog sistema, potpuno zanemaren.

Ekonomskim aspektima IB, sa stanovišta analize i upravljanja rizicima, bave se programski definisani modeli orijentisani na firme i biznis-procese.

3. ZAKLJUČAK

Informaciona bezbednost, kao vid bezbednosti, neodvojivi je deo informacionog društva. Sa istorijskim shvatanjem njenog značaja menjao se i pristup pitanju informacione bezbednosti.

Analizom datih modela uočava se sva složenost i kompleksnost pojma informacione bezbednosti kao i mogućnost različitih pristupa.

LITERATURA

1. Daniel G. Wolf, Statement before the House Select Committee on Homeland Security Subcommittee on Cybersecurity, Science and Research & Development, Nacional Security Agency US, Juli 22, 2003
2. Nacional Security Agency, Nacional Information Systems secutity Glossary, NSTISSI No 4009, Fort Meade, MD spt 2000
3. Field manuel No. 3-13, FM 3-13(FM 100-6) Information operations: Doctrine, Tactics, Technigues, and Procedures, Department of the Army, Washington, DC, nov 2003
4. Luiijf E., Information Assurance and the Information Society, EICAR Proceedings 1999
5. Панарин И., Н., Проблемы обеспечения информационной безопасности в савременных условиях, http://kiev-security.org.ua , 1997
6. Доктрина информационной безопасности Российсой Федерации, Президент, 09.09.2000, Пр-1895
7. Sinkovski S., Informaciona bezbednost – komponenta nacionalne bezbednosti, Vojno delo, 2/2005, str. 31-81
8. Maconachy V., Schou C., Ragsdale D., Welch D., A model for Information assurance: an integrated approach, Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security, United States Military Academy, West Point, 2001
9. Survivability – A New Technical and Business Perspective on Security, Proceedings of the 1999 New Security Paradigms Workshop. Caledion Hill, ON, sep 21-24, 1999, Nwe Jork, NY: Association for Computer Machinery, 2000
10. Леваков А., Анатомия информационной безопасности США, Jet info online # 6 (109), 2002
11. D. K. Hsiao, D.S. Kerr, S.E. Madnik, Computer security, Academic Press, New York, san Francisko, 1979
12. Rodić B., Interakcija javnih računarskih mreža i računarskih mreža specijalnih institucija *(doktorska disertacija)*, Vojnotehnička akademija, Beograd, 2001
13. Галатенко А.В., Основы информационной безопасности, Универзитет ИТ - ИНТУИТ.ru, 2004
14. А.Д.Урсул, Т.Н. Цырдя, Информационная безопасностъ, сущностъ, содержание и принципы ее обеспечения, журнал Факт № 2, 2000
15. П.В. Константинович, От информационных войн к управляемой конфронтации и сотрудничеству, журнал Факт № 9, 2001
16. Барсуков Д., Интегральная защита информации, "Электроника. Наука, технология, бизнес" № 3-4,1998г.
17. Beauregard J., Modeling information assurance, Air Force Institute of tehnology, 2001
18. Домарев В., Безопасностъ информационных технологий. Методология создания систем защиты, ДиаСофт, 2002

ENDNOTA:

[i] Reč je o saslušanju Daniela Wolfa pred podkomitetom za unutrašnju bezbednost senata SAD 22 jula 2003.godine. Daniel Wolf je direktor za informacionu garanciju (information assurance) u američkoj Agenciji za nacionalnu bezbednost (NSA – *Nacional Security Agency*).

[ii] Moguć je prevod: informaciona garancija, informaciona sigurnost, informaciono osiguranje ili, u nešto slobodnijem kontekstu, informaciono obezbeđenje.

[iii] Reč je o zaštitnim mogućnostima informacionih sistema da detektuju napad i da u slučaju uspešnog napada obnove osnovne funkcije.

[iv]Za razumevanje problema informacione bezbednosti u teoriji i praksi SAD neophodno je poznavati teoriju informacionog ratovanja.

[v] 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..

[vi] ISO/IEC 17799 Information security management – Code of Practice Information Security Management, BS 7799 Code of Practice Information Security Management, German Information Security Agency: IT Baseline Protection Manuel – Standard security safeguards, 2000.

[vii] Zakon RF "Об участии в международном информационом обмене"

[viii] Canadion Systems Security Centre, The Canadian trusted Computer Product Evaluation Criteria, Draft Version 3.0e, april 1992

[ix] Mrežni sistemi su računarske mreže koje povezuju različite korisnike povećavajući efikasnost organizacije na račun integracije (praćene povišenim nivom rizika) što računarske mreže čini kritičanim elemenatom modernog društva.

[x] «Virtuelne organizacije», nastale za rešavanje problema u složenim dinamičkim okolnostima, su informacioni, telekomunikacioni, računarski i kadrovski resursi organizovani po principu «informacionih matrica» koje omogućavaju fleksibilnu, bezbednu i centralizovanu raspodelu resursa.

[xi] Model je nastao kao rezultat napora Pentagona i Agencije za nacionalnu bezbednost SAD a proklamovan je u standardu ISO/IEC 15408.

[xii] Npr. ADDME - metod nazvan po prvim slovima njegovih etapa – ocena (*asses*), projektovanje (*design*), postavljanje (*deploy*), eksploatacija (*manage and support*) i obuka (*education*).

[xiii] Model ešelonirane višeslojne zaštite podrazumeva, na nivou nacionalne informacione ingrastrukture, prostornu i kiber-prostornu dubinu.

[xiv] Univerzitet informacionih tehnologija, Moskva

[xv] Podržavajuća infrastruktura podrazumeva sisteme elektro-, vodo- i toplotnog snabdevanja, kondicionere, sredstva komunikacija i, konačno, personal.

[xvi] В.Б.Бателu, В.А.Галатенко, Информационная безопасностъ с точки зрения технологиии программирования,

[xvii] A.D. Ursu (doktor filozofskih nauka, direktor Naučno-istraživačkog instituta stabilnog razvoja i bezbednosti, predsednik Međunarodne akademije Noosfere (stabilnog razvoja), akademik AN Moldavije i RAEN) i T.F. Cirdja (doktror filozofskih nauka, akademik Međunarodne akademije Noosfere, akademik Međunarodne akademije Informatizacije pri UN, akademik Ukrajinske akademije nauka, načelnik katedre filozofija i bioetika na GUMF im N.I. Testimicanu).

[xviii] Personal je podložan različitim vrstama informaciono-psiholoških delovanja.

[xix] Prema rečima R. Keeney, pionira VFT, formulisanje pravih vrednosti je osnova odlučivanja.

[xx] Ovaj model je rezultat istraživačkog rada na institutu tehnologije RV SAD u Air Force Tecnichal Center (AFTC).