UDC: 004.453 INFO M: str. 10 -17

INFORMACIONA SIGURNOST U SAVREMENOM SVETU
INFORTMATION SECURITY IN MODERN WORLD

Lazar D. Petrović

REZIME: U radu je učinjen pokušaj da se ukaže na značaj informacione sigurnosti u savremenom svetu. Informaciona sigurnost, kao novi pravac istraživanja u oblasti bezbednosti, ispoljava se i u oblasti nacionalne bezbednosti, ali i kao faktor međunarodnih odnosa. Nesumnjivo jedan od najvažnijih aspekata informacione sigurnosti je njen uticaj na celokupno društveno kretanje. Da je zaštita informacija predmet interesovanja državnih i vojnih struktura, poznato je od ranije. Međutim, i sve velike kompanije smatraju da je informaciona sigurnost jedan od najvažnijih prioriteta u vođenju biznisa. U skladu sa tim evidentne su radikalne promene u organizaciji službe informacione sigurnosti na svim nivoima. Pitanja informacione sigurnosti i problem zaštite informacija su sa, sve donedavno, krajnjih margina dospela u situaciju da budu delokrug rada samog top - menadžmenta kompanija.

KLJUČNE REČI: informaciona sigurnost, nacionalna bezbednost, zaštita informacija, aspekti informacione sigurnosti

ABSTRACT: In this paper, there made attempt to indicate on importance of information security in modern world. Information security, as a new way in security researching area, is detect in area of national security, as well as international relationships factor. Absolutely the most important aspect of information security is her influence on whole human movement. Its well knows from earlier time, that information protection was object of government and military structures. Also, all multi - companies consider that information security is one of the most important priorities in business management. According with this acknowledge, there made fundamental changes in organization of information security department, on whole levels. Not long ago, questions of information security and problem of information protection were on final margins and now, there is situation that top management companies use them in their work - spheres.

KEY WORDS: information security, national security, information protection, aspect of information security

1. UVOD

U poslednje vreme o informacionoj sigurnosti[1], u raznim varijantama, moguće je pročitati gotovo u svim svetskim časopisima. Da li je to posledica modnog trenda ili realna potreba u zaštiti informacija? Različite organizacije iz različitih razloga treba da štite svoje poslovne informacije. Za banke je od presudnog značaja **integritet** informacija, zbog finansijskog poslovanja, odnosno neizmenljivosti novčanih transakcija. Za provajdere Internet - usluga najvažnije su **raspoloživost** i **pouzdanost** informacija, zbog kontinuiteta u pružanju usluga, tj. dostupnost i pouzdan rad ključnih elemenata sistema. Za privrednike je pak najvažnija **poverljivost** informacija zbog opstanka na tržištu i uspešnog poslovanja, odnosno mogućnosti da informacijama pristupe samo ovlašćena lica. Za državne institucije su važni svi navedeni razlozi, pa čak i više od toga.

Poslovne informacije mogu oticati putem **tehničkih kanala** koji se u literaturi najčešće razmatraju kao kompjuterski kanali[2] ili putem tzv. **unutrašnjih kanala** gde spadaju saradnici sa svojim motivima i radnim navikama. Posledice neadekvatne zaštite informacija se mogu ogledati kao finansijski gubici, gubici u smislu smanjenja ugleda ili tržišnih pozicija itd., i kao takvi mogu imati katastrofalne posledice. Očiglednost potrebe za zaštitom informacija je posebno izražena u različitim oblicima elektronskog poslovanja (*e - business*).

Informaciona sigurnost je nov, složen i, u svojoj suštini, višeslojan pojam. Ona je predmet naučnih istraživanja u mnogim naukama, kako tehničko - tehnološkim (informatika, elektromagnetika, obrada signala) tako i humaniratnim (sociologija, psihologija, pravo, politologija).

Ovako shvaćena informaciona sigurnost ima široke implikacije na pravne, ekonomske i tehničke aspekte primene informaciono - komunikacionih tehnologija. U novom kontekstu shvatanja pojma bezbednosti, informaciona sigurnost je jedna od osnovnih komponenata nacionalne bezbednosti i osnova sigurnog i bezbednog poslovanja. Višedimenzionalnost i multidisciplinarnost informacione sigurnosti se svakako reflektuje na mnoge oblasti, pa između ostalog, i na planu međunarodnih odnosa.

2. ISTORIJSKI KONTEKST NASTANKA INFORMACIONE SIGURNOSTI

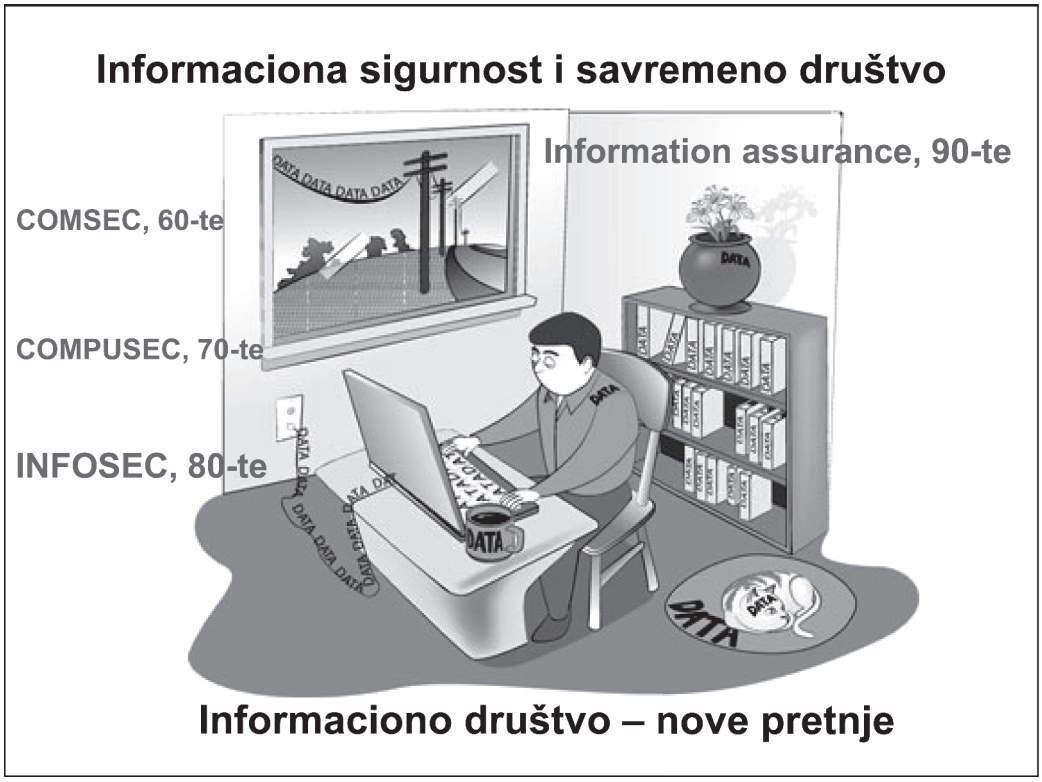
Primat u teoriji i praksi informacione sigurnosti pripada Sjedinjenim američkim državama. Kao osnovno polazište u savremenom definisanju pojmova u oblasti informacione sigurnosti poslužila je teorija informacionog ratovanja (IW - *information warfare*).

Prema rečima Daniela Wolfa[3] [4], istorijski posmatrano, prvo se pojavila, 60 - ih godina prošlog veka, komunikaciona sigurnost (COMSEC – *communication security*). Sa pojavom

[1] U radu se temini bezbednost i sigurnost koriste kao različiti sinonimi istog pojma, iako možda nije najkorektije, s tom razlikom da se za pitanja bezbednosti u informatičkoj sferi više koristi pojam sigurnost, jer je tako regulisano našim nacionalnim standardom SRPS ISO/IEC 17799, a u ostalim oblastima pojam bezbednost.

[2] Pojavom Interneta omogućeno je formiranje pogodne globalne komunikacione infrastrukture koja pruža mogućnost pristupa, u svetskim razmerama, firmama, kupcima, proizvođačima opreme i ključnim partnerima. Reč je o nesumnjivo proširenim mogućnostima međusobne razmene informacija i efikasnijeg poslovanja, ali i o povećanju rizika i opasnosti kada je u pitanju računarska mreža određene kompanije.

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



Slika 1. – *Istorijski razvoj pojma informacione sigurnosti*

kompjutera, 70 – ih godina, nastala je kompjuterska sigurnost (COMPUSEC – *computer security*). Krajem 80 – ih godina COMSEC i COMPUSEC su objedinjene u **informacionu sigurnost** (INFOSEC – *information security*) koja je pokušala da integriše ranije odvojene discipline kao što su sigurnost personala, kompjuterska sigurnost, komunikaciona i operativna sigurnost. 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 sigurnost je definisana kao: zaštita *informacionih sistema od neautorizovanog pristupa ili modifikacija informacija* bilo u postupku skladištenja, obrade ili prenosa i *onemogućavanja usluga autorizovanim korisnicima, uključujući neophodne mere detektovanja, dokumentovanja i otklanjanja takvih pretnji* [2].

Napredak u kompjuterskoj tehnici i pojava računarskih mreža (LAN i WAN i, pre svega, INTERNET - a), proširuje listu svojstava informacija, pred koje se postavljaju bezbednosni 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**[4] (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 dve važne karakteristike, a to su *operativnost* (*operational in nature*) i *osetljivost na vreme* (*time – sensitive*). Ove karakteristike izražavaju termini detekcija (*detection*) i reakcija (*reaction*)[5]. Reč je o defanzivnim operativnim mogućnostima koje se, zajedno sa tradicionalnim informaciono – garancijskim aktivnostima, od kasnih 90 – ih godina opisuju terminom teorije informacionog ratovanja – odbrambenih informacionih operacija (DIO - *defensive information operations*)[6] [4,6].

Konačno 2002. godine direktivom Ministarstva odbrane SAD (DoDD Number 8500.1 *Information assurance*, octobar 24, 2002), zvanično je uveden pojam *informaciona garancija* ili informaciono obezbeđenje.

Informaciona garancija je definisana kao ‘’*informaciona operacija 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* [7].

Evropske zemlje, u svom shvatanju pojma informacione sigurnosti, sa naglašenijim pragmatičnim pristupom[8], uglavnom prate poglede SAD [1].

[4] Moguć je prevod: informaciona garancija, informaciona sigurnost, informaciono osiguranje ili, u nešto slobodnijem kontekstu, informaciono obezbeđenje.
[5] Reč je o zaštitnim mogućnostima informacionih sistema da detektuju napad i da u slučaju uspešnog napada obnove osnovne funkcije.
[6] Za razumevanje problema informacione sigurnosti u teoriji i praksi SAD neophodno je poznavati teoriju informacionog ratovanja.
[7] 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.
[8] 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.

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

Informaciona sigurnost je, u doktrinarnim dokumentima Ruske federacije, 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*[9]. Kao polazno stanovište pri definisanju pojma uzet je interdisciplinarni pristup, odnosno, opšta nauka o bezbednosti.

U "*Doktrini informacione sigurnosti Ruske federacije*" termin informaciona sigurnost koristi se u širem smislu, dok je u zapadnim shvatanjima reč o užem smislu pojma, jer se odnosi samo na informacije i informacione sisteme.

U okviru tzv. "ruske škole" razlikuje se nekoliko predstavničkih pravaca: predstavnici humanitarnih nauka koji ostaju na nivou opštosti (konceptualni modeli informacione sigurnosti), predstavnici bliski zapadnim gledištima i predstavnici 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 sigurnost je disciplina u okviru informacionih tehnologija i predstavlja njenu osnovnu komponentu.

U Srbiji problematika informacione sigurnosti nije, kao takva, dovoljno razmatrana. Pod terminima *zaštita informacija*, *bezbednost i zaštita informacija* ili *zaštita podataka* tretirani su neki od aspekata informacione sigurnosti, uglavnom sa istorijski prevaziđenih stanovišta.

Činjenica da je, prema savremenim shvatanjima pojma nacionalne bezbednosti, informaciona sigurnost jedna od njenih osnovnih komponenti, to problematiku informacione sigurnosti čini krajnje aktuelnom [1].

3. NACIONALNA I INFORMACIONA SIGURNOST

Nacionalna bezbednost predstavlja deo ukupnog *sistema nacionalne bezbednosti* koji čine *objekti bezbednosti*, nad kojima se provode bezbednosne operacije, *subjekti* preko kojih se obezbeđuju mere bezbednost i *mehanizmi bezbednosti* u skladu sa kojim se realizuju praktične bezbednosne akcije. *Osnovni objekti bezbednosti* ili zaštite su: ličnosti – njihova prava i slobode, društvo – njegove materijalne i duhovne vrednosti i država – njeno konstitucionalno uređenje, suverenitet i teritorijalna celovitost. *Subjekti* koji obezbeđuju i provode sistem bezbednosti su: organizacije, državne institucije, službe i samostalne ličnosti. *Mehanizmi* kojima se realizuje sistem bezbednosti definišu dinamičku šemu obezbeđenja nacionalne bezbednosti kroz skup mera, akcija i postupaka [9].

Sistem nacionalne bezbednosti predstavlja sveukupnost objekata bezbednosti sa izbalansiranim životnovažnim interesima, subjekata bezbednosti sa njihovim funkcijama, pravima, odgovornostima, obavezama, oblastima kompetentnosti, sredstvima obezbeđenja bezbednosti u različitim sferama delatnosti i odnosima između njih, u skladu sa kojima se reguliše, planira, organizuje, koordinira, sinhronizuje i kontroliše svrsihodna delatnost postizanja i održavanja stanja bezbednosti adekvatna unutrašnjim i spoljašnjim pretnjama, životnovažnim interesima ličnosti, društva i države [13].

U osnovi opštih *nacionalnih interesa* se nalazi čovek, porodica i društvo, njihova prava, slobode i garancija nesmetanog razvoja. Važni nacionalni interesi su: napredak i razvoj čoveka kao jedinke, poboljšavanje kvaliteta života, lična i društvena bezbednost, očuvanje suvereniteta, teritorijalnog integriteta zemlje i njenog državnog uređenja, jedinstvo ekonomskog tržišta i ekonomski rast i garantovana državna sloboda demokratskog razvoja društva, očuvanje građanskog mira, društvenog poreka i nacionalne saglasnosti [9].

Informaciona sigurnost, shvaćena u najširem značenju reči[10], ne samo da dobija na značaju, već izbija u prvi plan nacionalne bezbednosti. Kao takva ona je *neodvojivi deo nacionalne bezbednosti* i u sve većoj meri poprima i međunarodni karakter, jer je celovitost savremenog sveta, kao društva, zasnovana na intenzivnoj razmeni informacija. *Elementi informacione sigurnosti*, u kontekstu nacionalne bezbednosti, su: informaciono pravo kao pravna osnova informacionog društva, informacioni aspekt upravljanja vojnim snagama i oružjem, informaciono ratovanje i informaciona protivodbrana, elektronsko ratovanje kao borba za dominaciju u elektromagnetnom spektru, informaciona sigurnost informacionih sistema i zaštita informacija, zaštita državne tajne, izviđanje i služba izviđanja, informaciono - psihološka protivodbrana i psihološko ratovanje, informaciono - psihološka sigurnost i moralno - psihološko obezbeđenje stanovništva, oružanih snaga i drugih vojnih i državnih organizacija [9].

Nacionalna bezbednost**,** prema shvatanjima u Ruskoj federaciji, je osnova stabilnog postojanja i progresivnog razvoja države u svetskoj zajednici. Ona predstavlja *stanje zaštićenosti životno važnih interesa ličnosti, društva i države, odnosno nacionalnih interesa, od spoljašnjih i unutrašnjih pretnji* [8].

Zvanični pogledi Ruske federacije na nacionalnu bezbednost izloženi su u ''*Koncepciji nacionalne bezbednosti*'', izdate 2000. godine.

U shvatanju pojma nacionalne bezbednosti SAD polazi se od staništa da pored pretnji spolja (druga ili druge države), postoje i unutrašnje pretnje, kao što su terorizam, elementarne nepogode, narušavanje ljudskih prava itd., koje su, po mnogo čemu, i veće i opasnije od spoljašnjih. U skladu sa tim pored ''*Strategije nacionalne bezbednosti*'' (*National Security Strategy,* iz 2002. godine) postoji i ''*Nacionalna strategija unutrašnje bezbednosti*'' (*National Strategy for Homeland security*, takođe iz 2002. godine). Činjenica da kao osnovna

[9] Zakon Ruske federacije "Об участии в международном информационом обмене"

[10] Informaciona sigurnost je definisana kao sigurnost informacionih sistema i zaštita informacija, a ne kao bezbednost imanentna informacionom društvu.

pretnja SAD figuriše terorizam, ne umanjuje značaj suštinski nove ideje, da unutrašnja bezbednost ima objektivno mnogo veći značaj i da se *nacionalna bezbednost tretira na novi način*.

Za razliku od Ruske federacije u kojoj je zastupljen, istina inoviran ali ipak, na tradicionalan način izložen problem nacionalne bezbednosti, SAD, sa stanovišta neospornog svetskog lidera koji, osim elementarnih nepogoda, ima samo jedan realan problem, a to je međunarodni terorizam, problemu nacionalne bezbednosti pristupa se iz jednog drugog ugla gledanja, tj. sa stanovišta zaštite svoje infrastrukture[11].

Još od 90 - ih godina rukovodeći krugovi u SAD su pokazivali zabrinutost zbog pojave novih pretnji nacionalnoj bezbednosti. Posle Prvog zalivskog rata, zbog sve češće upotrebe pojmova ''informaciono ratovanje'' i ''informaciono oružje'', Ministarstvo odbrane izdalo je direktivu TS 3600.1 od 21. decembra 1992. godine, pod nazivom "*Informaciona protivodbrana*" u kojoj je ukazano na neophodnost vođenja računa o informacionim resursima pri organizaciji planiranja i funkcionisanjasistemaupravljanja,uciljupovećanjaefektivnosti dejstava vojnih snaga u uslovima protivdejstava protivnika. Od tog vreme intenzivno se radi na zadacima istraživanja i razvoja "borbe sa sistemima upravljanja", sa osnovnim ciljem ostvarivanje informacione superiornosti. Već 1993. godine Komitet združenog generalštaba donosi memorandum MOP - 30 sa detaljnim konceptom borbe sa sistemima upravljanja. Godine 1994. slede publikacije Komiteta za nauku Ministarstva odbrane SAD o specijalnim organizaciono - tehničkim merama zaštite informacione infrastrukture. U februaru 1996. godine KoV SAD izdaje FM - 106 ''*Informaciona operacija*'' (*Information operations, 1996*), a 1998. godine usledila je direktiva za zaštitu kritične infrastrukture, PDD - 63 (*Critical Infrastructure Protection*) da bi, kao konačan sled zbivanja, usledio početkom 2000. godine ''*Nacionalni plan zaštite informacione infrastrukture*'' (*National critical infrastructure plan, 2000*). Praktično sa ovim Planom počinje nova inicijativa administracije SAD u oblasti nacionalne bezbednosti. Taj plan predstavlja sveobuhvatno gledanje na probleme zaštite ključnih sektora nacionalne ekonomije, nacionalnu bezbednost, opštu zdravstvenu zaštitu i ličnu bezbednost građana.

Plan sadrži 10 nezavisnih programa objedinjenih jednim opštim ciljem. Važna teze Plana je konsolidacija napora vlade, federalnih ministarstava i privatnog sektora u zaštiti informacione infrastrukture kao najvažnijeg nacionalnog resursa. Programi koji su obuhvaćeni ovim planom su:

1. *Definisanje kritično važnih resursa infrastrukture*, njihovih uzajamnih veza i pretnji koje stoje pred njima;
2. *Detekcija napada* i neovlašćenih upada u kompjuterske sisteme;
3. Razrada *delovanja obaveštajne službe i donošenje pravnih akata*;
4. Blagovremena *razmena informacija* o napadima;
5. *Dizajniranje sredstava reagovanja*, rekonfiguracije i rekonstrukcije;
6. Aktiviranje *naučno - istraživačkih zadataka* na podršci programa 1 do 5;
7. Priprema i raspodela neophodnog broja *specijalista* u oblasti informacione sigurnosti;
8. *Informisanje* američkog društva o neophodnosti progresa na planu informacione sigurnosti;
9. Donošenje dopuna i *izmena u zakonodavstvo* u interesu programa 1 do 8 i
10. Obezbeđenje zaštite *građanskih sloboda* svih amerikanaca [2, 10].

Pregled programa ''*Nacionalnog plana zaštite informacionih sistema*'' pokazuje ozbiljne namere SAD da problem informacione sigurnosti, a samim tim i nacionalne bezbednosti, rešava na novi način. U centar svih razmatranja postavlja se pitanje kritične infrastrukture, a ona je, po prirodi informacionog društva, informaciona struktura. S druge strane, problem informacione sigurnosti je podignut na opštenacionalni nivo pri čemu je svaki građanin ne samo korisnik koji brine o ličnoj bezbednosti, već i o bezbednosti društva u celini.

Pojam *kritična infrastruktura* je definisan u zakonu ''O patriotizmu'' (*USA Patriot Act of 2001*, October 2001), kao ''*sveukupnost fizičkih ili virtuelnih sistema i sredstava važnih za SAD u toj meri da njihovo izbacivanje iz stroja ili unuštavanje može dovesti do fatalnih posledica u oblasti odbrane, ekonomije, očuvanja zdravlja i bezbednosti nacije*''. Kritičnu infrastrukturnu čine javne i privatne institucije u sektorima poljoprivrede, prehrane, vode, zdravstva, hitnih službi, vlade, odbrane, informacija i telekomunikacija, energetike, saobraćaja, bankarstva i finansija, hemijskih i opasnih materijala, pošte, špedicije i drugo.

Unutrašnja bezbednost, kao deo nacionalne bezbednosti SAD, regulisana je zakonom ''*O unutrašnjoj bezbednosti*'' (*Home Security Act, H.R, 5005,* 25. 11. 2002.). Za praćenje njegovog sprovođenja nadležan je Komitet za unutrašnju bezbednost (*House Homeland Security Committee*). U okviru njega, za pitanja ''*Kiber bezbednosti, nauke, istraživanja i razvoja*'' (*House Homeland Security subcommittee on Cybersecurity, Science and Research and development),* formiran je podkomitet koji se bavi ''*bezbednošću kompjuterskih i komunikacionih mreža, informacionih tehnologija, sistema upravljanja proizvodnjom, sistemom elektrosnabdevanja i bazama podataka, kako vladinih tako i privatnih, od unutrašnjih i spoljašnjih napada predupređujući gubitke stanovništva i infrastrukture*'' [12]. Kako je kiberprostor[13] *nervni sistem,* odnosno upravljački sistem SAD, od koga zavisi ekonomija i nacionalna bezbednost zemlje, to je 2003. godine donešena ''*Nacionalna strategija bezbednosti kiber prostora*'' (*The Nacional Stategy to secure Cyberspace, feb 2003*).

[11] Predsednička komisija o zaštiti kritične infrastrukture (PCCIP - Presidents Commission on Critical Infrastructure Protection, 1997) je došla do zaključka da je informaciono - komunikaciono tehnološka infrastruktura (ITC – information and communication technology infrastructure) osnovna prednost društva koju treba da zaštiti zajedno kao i vojna i civilna odbrambena politika i sredstva (E.Luiijf, Information assurance and the information society,1999)

[12] Leadership selected for new cybersecurity panel GCN, By William Jackson, 03/21/03

[13] Kiberprostor se sastoji od stotina hiljada međusobno povezanih kompjutera, servera, rutera, svičeva i fiber optičkih kablova koji omogućavaju određenim infrastrukturama da funkcionišu [12].

Međutim, osnovni nosilac posla u oblasti unutrašnje bezbednosti je novoformirano ministarstvo - *Ministarstvo unutrašnje bezbednosti* (*Depertment of Homeland Security*). Pri formiranju ministarstva pošlo se od shvatanja da je bezbednost države neodvojiva od bezbednosti građana. U tom smislu su njegove osnovne funkcije: sprečavanje terorističkih napada, smanjenje ranjivosti SAD na terorističke akcije, smanjenje posledica terorizma, eliminisanje posledica tehnogenih, antropogenih i prirodnih katastrofa, sagledavanje ekonomskih interesa SAD u sklopu mera unutrašnje bezbednosti, borba protiv narkomafije i njenih veza sa terorizmom i druge funkcije koje nisu direktno vezane za unutrašnju bezbednost [11].

Ministarstvo čine 4 direktorata koji se bave pitanjima:

- *analize informacija i zaštita infrastrukture* (*Information Analisys and Infrastructure Protection*),
- *bezbednosti granica i transporta* (*Border and Transportation Security*),
- *pripravnosti za vanredno stanje i reagovanje* (*Emergency Preparednes and response*) i
- *nauke i tehnologije* (*Science and Technology*).

Unutar Ministarstva, posebno mesto pripada prvom direktoratu koji objedinjava analizu obaveštajno - izviđačkih informacija o terorističkim pretnjama (što je povuklo za sobom reorganizaciju obaveštajno - izviđačke službe SAD) i zaštitu kritične infrastrukture. Interesantno je napomenuti da su sve funkcije unutrašnje bezbednosti ''pokrivene'' normativnim dokumentima. Tako je već 2003. godine donešeno nekoliko strategija: ''*Nacionalna strategija borbe sa terorizmom*'' (*The Nacional Stategy for Combating Terrorism*), ''*Nacionalna strategija bezbednosti kiber prostora*'' (*The Nacional Stategy to secure Cyberspace*) i ''*Nacionalna strategija fizičke zaštite kritične infrastrukture*'' (*The Nacional Stategy for the Physical Protection of Critical Infrastructures and Key Assets*).

Nove strategije, po prvi put oficijalno, priznaju potpunu zavisnost infrastrukture SAD od informacionih sistema i mreža i zahtevaju od svih društvenih činilaca (javnog i privatnog sektora) formiranje *Jedinstvenog nacionalnog sistema reagovanja na kiber napade* (*National Cyberspace Security response System)*. Nacionalni program saradnje u oblasti informacione sigurnosti (*The National Information Assurance Partnetship* - NIAP) prisutan je još od 1997. godine. Neaktivnost lokalnih organa, ali i sama priroda problema je dovela do toga da vlada SAD preuzme sve prerogative u ovoj oblasti. I naravno donešeni su odgovarajući zakoni: ''*Zakon o povećanju kiber sigurnosti*'' (*Cyber Security Enhancment Act of 2002*, H.R.3482), ''*Zakon o finansiranju obaveštajne delatnosti u 2003*'' (*Intelligence Authorization Act For Fiscal Year 2003*) i ''*Zakon o razmeni informacija u interesu unutrašnje bezbednosti*'' (*Homeland Security Information Sharing Act*, 2003).

Posledica novih shvatanja datih u strategijama, direktivama i zakonima su: rad na razvoju nacionalnog sistema veza[14] (*National Communications System* - NCS), reorganizacija obaveštajno - izviđačke službe (*intelligence community*), fizička zaštita važnijih objekata kritične infrastrukture, insistiranje na ključnoj ulozi informacionih tehnologija u povećanje unutrašnju bezbednosti[15], podrška tehnološkoj nadmoći SAD, istraživanje u oblasti zaštite informacione infrastrukture[16] i obuka građana u sticanju navika preživljavanja u uslovima tehnogenih i prirodnih katastrofa i terorističkih napada.

Novi pristup rešavanju pitanja unutrašnje bezbednosti, u uslovima globalizacije, ne deluje samo na američko društvo, već se odražava i na ostala društva[17]. Network - centric paradigma, zasnovana i još uvek prisutna samo u SAD, preliće se i na ostale zemlje sveta, a ona podrazumeva visok stepen zavisnosti bezbednosti nacionalne informacione infrastrukture od informacione sigurnosti svih njenih elemenata, kako državnog tako i privatnog sektora. Na taj način, informaciona sigurnost bilo koje kompanije postaje faktor nacionalne i unutrašnje bezbednosti države u celini. *Izgradnja efektivne bezbednosne infrastrukture*, tzv. integrisane informacione infrastrukture (III – *integrated information infrastructure*), *nije pitanje dobre volje, već stvar nacionalne bezbednosti zemlje*.

4. INFORMACIONA SIGURNOST U SJEDINJENIM AMERIČKIM DRŽAVAMA

O značaju koji se pridaje informacionoj sigurnosti u SAD svedoči struktura upravljanja bezbednošću informacione infrastrukture (slika 2.). Pored državnih institucija, važno mesto zauzimaju i naučne institucije. Tako su, u strukturu upravljanja, neposredno uključena dva naučna instituta: *Insitut zaštite informacione infrastrukture* I^3P i *Nacionalni institut standarda i tehnologija* NIST i pet centara: *Federalni centar zaštite informacione infrastrukture* FedCIRC, *Nacionalni centar zaštite informacione infrastrukture* NIPC, *Nacionalni centar bezbednosti i reagovanja* NSIRC, *Centar za analize informacija* ISAC i *Centar za zaštitu informacione infrastrukture federalnih agencija i ministarstava*.

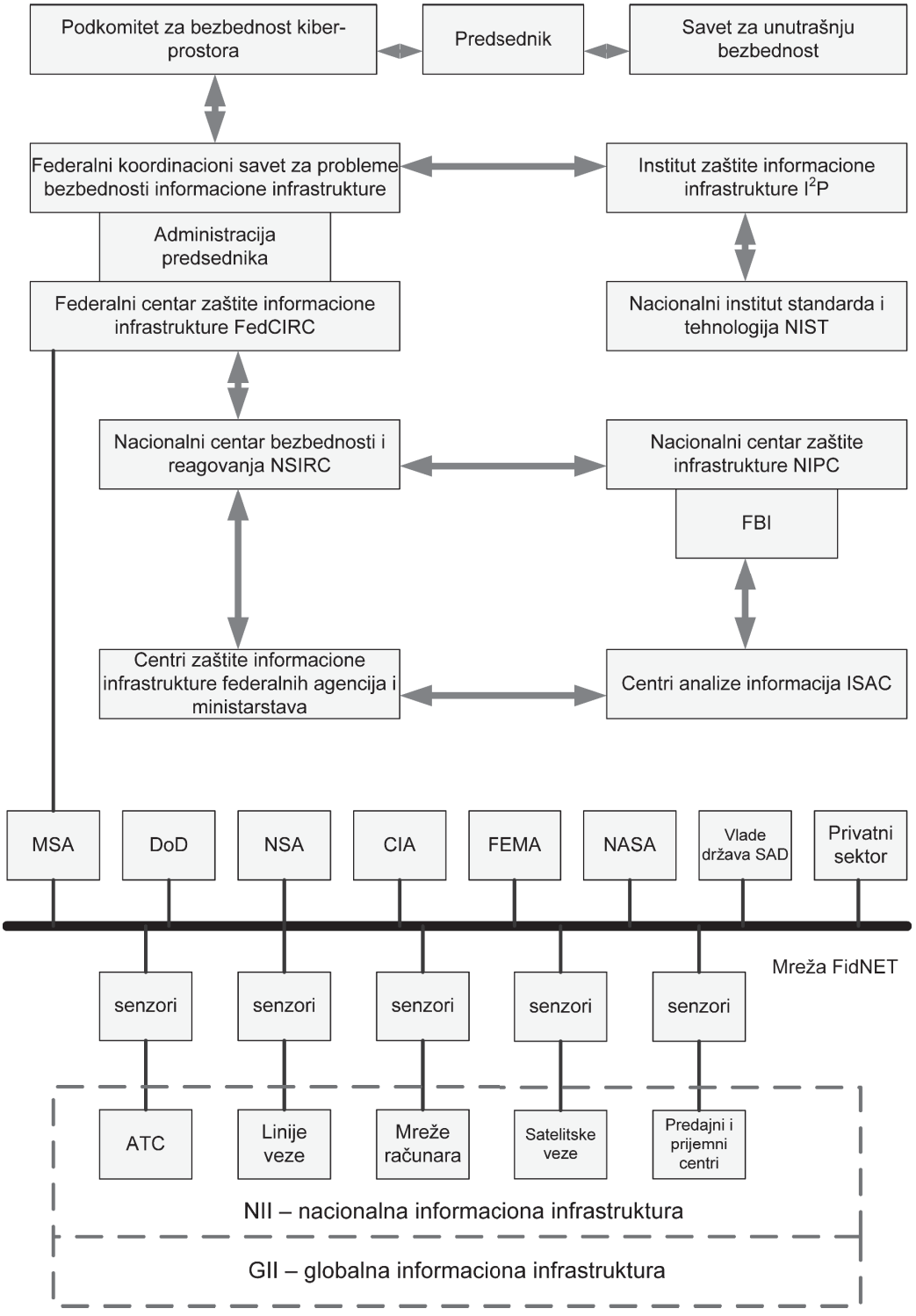
Svi američki univerziteti, počev od Univerziteta nacionalne odbrane UND, u svom sastavu imaju fakultete informacione sigurnosti. *Naučno - istraživačka delatnost* definisana je sa

[14] Vruća linija (Emergency response Link - ERLink), perspektivna inteligentna mreža (Advanced Intelligent Network - AIN), mreža upozorenja i koordinacije (Alerting and Coordination Network - ACN), vladin telekomunikacioni servis u vanrednim prilikama (Government Emergency Telecomminications Service - GETS), nacionalni koordinacioni centar (National Coordinating Center - NCC), razmena informacija o resursima veze (Communications Resource Information Sharing - CRIS), distribuirani resursi (Shares Resources - SHARES), prioritetni telekomunikacioni servis (Telecommunications Service Priority - TSP), bežični prioritetni servis (Wireless Priority Service – WPS) i obuka, planiranje i tehnička podrška (Training, Planing and Operational Support - TPOS).

[15] Informacione tehnologije će igrati ključnu ulogu u povećanju unutrašnje bezbednosti nacije pred budućim potencijalnim opasnostima. U suštini, informacione tehnologije će pomoći naciji da odredi potencijalne pretnje, da operativnije distribuira informacije, da obezbedi mehanizme zaštite zemlje i razradi odgovarajuće protivmere (Homeland Security – Information Technology Funding and Associated Management Issues, GOA-03-250, decembar 2002).

[16] Perspektivne oblasti istraživanja i razvoja: upravljanje bezbednošću kompanija, bezbednost distribuiranih autonomnih grupa, istraživanje bezbednosti i analiza ''ranjivih'' mesta, rekonstrukcija bezbednosti sistema i mreža, bezbednost bežičnih sistema, pokazatelji i modeli i pitanja zakonodavstva, politike i ekonomije (Cyber security research and development agenda, Institut for information infrastructure protection, January 2003).

[17] Tako npr. već 11. 03. 2003. godine izvršena je reorganizacija ruskih specijalnih službi [1].



Slika 2. – *Struktura upravljanja u oblasti bezbednosti nacionalne informacione infrastrukture SAD*

prvih pet programa *Nacionalnog plana zaštite informacione infrastrukture* (2000. god.) i pet nacionalnih prioriteta u oblasti zaštite informacione infrastrukture, defisanih *Nacionalnom strategijom bezbednosti kiber prostora* (2003. god.).

Zaštita informacione infrastrukture je predmet živog interesovanja u SAD. Tako npr. Insitut za zaštitu informacione infrastrukture[18], koji čine 23 državne organizacije, je na osnovu opsežnih ispitivanja, izdao listu prioritetnih istraživanja u ovoj oblasti, koja se ogleda u sledećem:

- upravljanje u oblasti bezbednosti kompanija,
- bezbednost distribuiranih autonomnih grupa,
- ispitivanje bezbednosti i analiza ranjivosti,

[18] I3P – Insitut Information Infrastructure Protection

- mogućnost regeneracija sistema i mreža,
- pitanje identifikacija,
- bezbednost bežičnih sistema,
- kriterijumi i modeli (zasnovanost investicija i dozvoljeni nivo rizika) i
- pitanja zakonodavnih, političkih i ekonomskih aspekata informacione sigurnosti [6].

Pored naučnih institucija, problematikom informacione sigurnosti se bave i neke druge institucije koje objedinjavaju teoretska i praktična istraživanja. Najpoznatije insitucije ovog tipa su koordinacioni centri – timovi za odgovor CERT/CC (*computer emergency response team*), CIAC (*computer incident advisory capability*) i FIRST (*forum of incident response and security teams*). Ove institucije prikupljaju statističke podatke o napadima i ranjivostima hardvera i softvera, pronalaze efikasne odgovore za protivdejstva i publikuju ih u svojim biltenima [7].

Koordinacioni centar CERT/CC se nalazi u Pitsburgu (Pensilvanija). Osnovalo ga je Ministarstvo odbrane SAD 1988. godine posle pojave ‘’crva” Moris. Osnovni cilj postojanja je razrada tehnologija i metoda protivdejstava, kao i analiza napada i minimizacija gubitaka. Periodično CERT publikuje tzv. Advisories – opis ranjivih mesta i način njihovog eliminisanja. Zbornik saveta se može naći na Web - serveru http://www.cert.org i FTP - serveru ftp://ftp.ert.org/pub/cert advisories. Informacije o problemima bezbednosti i njihovom rešavanju, koja se dobijaju od proizvođača, publikuju se u specijalnim biltenima Vendor - Initiated Bullitens. Danas je CERT jedan od najpoznatijih centara, sa preko 40 predstavništava u svetu.

Zbog nemogućnosti okupljanja specijalista za sve oblasti informacione sigurnosti, pristupilo se formiranju i drugih centara kao što su CIAC i FIRST. CIAC je organizovan pri Ministarstvu energetike 1989. godine, čija je osnovna funkcija izveštavanje o incidentima, obezbeđenje informacione sigurnosti ministarstava, organizovanje simpozijuma i konsultacija o pitanjima informacione sigurnosti, itd. I centar CIAC publikuje informacioni bilten (Advisories) na svom Web - serveru llnl.ciac.gov.

FIRST je formiran kao centar za koordinaciju između postojećih centara 1990. godine. On predstavlja međunarodni forum koji objedinjava sva grupna reagovanja na incidente. Sredinom 1997. godine u okviru FIRST - a je bilo oko 60 timova iz različitih zemalja. Osnovni zadaci FIRST - a su saradnja među učesnicima foruma, zajednički rad na istraživačkim zadacima i obaveštavanje korisnika o mehanizmima informacione sigurnosti. FIRST organizuje svake godine simpozijum *Computer security incident handling workshop* za sve zainteresovane i 2 do 3 puta godišnje kolokvijume za svoje učesnike.

U skladu sa federalnim zakonima, zakonom *Computer security act* (1987) i instrukcijom OMV A -130, NASA je formirala svoj centar NASIRC (*NASA automated systems incident response capability*). Njegov zadatak je informaciona sigurnost odeljenja NASE. NASIRC ulazi u sastav FIRST - a.

Federalni centar zaštite informacione infrastrukture FedCIRC (*Federal Computer Incident Response Capability*) je osnovan krajem 1996. godine od strane NIST, CERT i CIAC. Ovaj centar obezbeđuje informacijama federalne nevojne organe vlasti [7].

Godine 1994., jedan od organizatora CERT/CC – Kristofer Klaus, osnovao je kompaniju ISS (*Internet Security Systems*) koja je lider u oblasti proizvodnje sredstava za analizu zaštićenosti i detekcije napada. U kompaniji ISS postoji naučno - istraživačka grupa X – force, koja okuplja eksperte u oblasti informacione sigurnosti. Ova grupa ne samo da prati publikacije drugih grupa, već i sama vrši testiranja softverskih i hardverskih proizvoda. Rezultati tih ispitivanja se nalaze u bazi podataka na adresi www.iss.net/xforce koja predstavlja jednu od najboljih baza podataka po pitanjima analize ranjivosti informacionih sistema. Ova baza je sastavni deo sistema analize zaštićenosti mrežnih servisa i protokola - Internet Scanner, sistema detekcije napada - RealSecure, sistema zaštićenosti operacionih sistema - System security Scanner i Security Manager i sistema za analizu zaštićenosti baza podataka - Databuse Scanner.

Kada je reč o informacionoj sigurnosti, u SAD, treba reći i to da postoji tesna saradnja državnog i privatnog sektora što je definisano i u svim doktrinarnim dokumentima.

4. INFORMACIONA SIGURNOST U RUSKOJ FEDERACIJI

Ruska federacija nema razgranatu strukturu upravljanja informacionom sigurnošću kao što je to u SAD. U okviru Saveta bezbednosti Ruske federacije formirani su naučni savet, koji u svom sastavu ima sekciju za informacionu sigurnost i međuuredsku komisiju za pitanja informacione sigurnosti. Naučnim radom u oblasti informacione sigurnosti rukovodi Naučni savet preko zajednice univerziteta Rusije. Na moskovskom državnom univetzitetu (MGU) Lomonosov, 2004. godine formiran je Institut za probleme informacione sigurnosti, IPIB (*Институт за Проблем Информационной Безопасности*), kao i Akademija za kriptografiju, RAK (*Росская Академий Крипторафии*).

Sekcija za informacionu sigurnost, pri Savetu bezbednosti Ruske federacije, je odobrila projekte, koji su objavljeni u protokolu N 1, od 28. marta 2001. godine, i to:

- "*Osnovni pravci naučnih istraživanja u oblasti informacione sigurnosti Ruske federacije*" i
- "*Prioritetni problemi naučnih istraživanja u oblasti informacione sigurnosti Ruske federacije*".

U spisku prioritetnih problema za humanitarne probleme su predviđena 33 zadatka, a za fizičko - matematičke i tehničke probleme – 41 zadatak. Navedenim dokumetima je definisano i 10 zadataka u sferi obrazovanja.

Institut za probleme informacione sigurnosti (IPIB) čine tri odeljenja:

– odeljenje matematičkih problema informacione sigurnosti,

– odeljenje informacione sigurnosti kompjuterskih sistema i

– odeljnje humanitarnih problema informacione sigurnosti.

Naučna istraživanja prva dva odeljenja baziraju se na bogatoj tradiciji matematičkih škola moskovskog univerziteta. Zadatak ovog Insituta je, pored ostalog, podrška i razvoj kriptografske škole

Osnovna istraživačka tematika **odeljenja matematičkih problema informacione sigurnosti** su *kriptografija* i *kriptologija*. Zadaci odeljenja su pretežno teoretskog karaktera, ali je ostavljena mogućnost korišćenja dobijenih rezultata u praktičnim primenama.. U okviru matematičkih problema predmet istraživanja je i *steganografija*. U toj oblasti razrađuje se niz važnih zadataka savremenih problema informacione sigurnosti, kao npr. zaštita intelektualnesvojineudigitalnomsvetu,idrugo.

Odeljenje informacione sigurnosti kompjuterskih sistema se bavi *matematičkim i softverskim obezbeđenjem informaciono - računarskih i mrežnih tehnologija nove generacije.* Ovo je ujedno i jedna od novih specijalnosti posdiplomskih studija, gde se izučava kompleksni pristup rešenju informacione sigurnosti, zavedena pod oznakom 05.13.11. Osim ovog, u ovom odeljenju se istraživači bave i tehnologijom projektovanja distribuiranih informaciono - računarskih sistema, upravljanjem velikim i supervelikim bazama podataka, logičko - jezičkim sredstvima upravljanja automatizovanim biznis - procesima i superbrzim računarskim sistemima sa masovnim paralelizmom.

Jedan od osnovnih istraživačkih pravaca ovog odelenja je i pronalaženje matematičkog modela zaštite distribuiranih informaciono - računarski sistema, jer su se svi dotadašnji modeli odnosili isključivo na mono sisteme. Institut se prihvatio pronalaženja *modela zaštite megakompjuterskih sistema koji se mogu sastojati od različitih segmenata sa različitim politikama u rešavanju pitanja bezbednosti.* Trenutno se radi na matematičkom modeliranju politike bezbednosti sa pristupom na osnovu uloga. Ovakav model omogućava teorijsko obrazloženje garancije zaštite podataka pri bilo kojoj konfiguraciji distribuiranih sistema. U tesnoj vezi sa ovim istraživanjima je i istraživanje u oblasti grid – tehnologija, tj. mrežne tehnologije. Posebna oblast istraživanja su sistemi za detekciju napada i postupci operativnog reagovanja, na osnovama modela mnogoagentnih napada na izazivanje otkaza u opsluživanju, sa mogućnošću korišćenja skrivenih kanala veze.

Treće odeljenje, **odeljnje humanitarnih problema informacione sigurnosti**, se bavi potpuno novim oblastima informacione sigurnosti – *humanitarnim problemima*. Zadatak ovog odeljenja je koordinacija ispitivanja psiholoških i sociolških aspekata bezbednosti. Suština ovih ispitivanja je psihologija ponašanja ljudstva u mreži, psihologija hakera, uzroci pojave hakerstva, psihologija odnosa deteta i kompjutera i razrada metodologije sprečavanja kiberhuliganstva. U ovom odeljenju se radi na razrešavanju pravnih pitanja povezanih sa digitalnim potpisom, elektronskom razmenom dokumenata i problemima rešavanja kompjuterskih prestupa.

5. ZAKLJUČAK

Informaciona sigurnost, kao vid sigurnosti, neodvojivi je deo informacionog društva. Sa istorijskim shvatanjem njenog značaja menjao se i pristup pitanju informacione sigurnosti. Savremeno informaciono društvo je nezamislivo bez ozbiljnog teritanja informacione sigurnosti. Analiza metoda ispitivanja i nekih od modela informacione sigurnosti ukazuje na svu složenost i kompleksnost pojma informacione sigurnosti kao i mogućnost različitih pristupa toj problematici.

LITERATURA

[1] Леваков А., Анатомия информационной безопасности США, Jet info online # 6 (109), 2002

[2] Леваков А., США принят план защиты информационных систем, Jet Info № 8/2000

[3] Лукацкий А.В., Взгляните на безопасностъ своей сети глазами специалистов, журнал «Мир Интернет», № 2, 1999.

[4] 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

[5] Доктрина информационной безопасности Росскийой Федерации, Президент, 09.09.2000, Пр-1895

[6] Nacional Security Agency, Nacional Information Systems secutity Glossary, NSTISSI No 4009, Fort Meade, MD spt 2000

[7] 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

[8] Концепция националъне безопасности**,** ukaz predsednika № 1300 iz 1997 i redakcija № 24 iz 2000)

[9] Основы националъной безопасности**,** prikaz knjige Б.А.Демидова „Концептуалъные основы и елементы националъной безопасности“, http://domarev.ru

[10] J. Miteff, Critical infrastructure: background, policy, and iplementacion, CRS report for Congres, 4. feb 2002

[11] Protecting the Homeland, report of the Defense science board, 2001

[12] 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

[13] D. K. Hsiao, D.S. Kerr, S.E. Madnik, Computer security, Academic Press, New York, san Francisko, 1979

[14] Медведовский И., Современные методы и средства анализа и контроля рисков информационных систем компаний, Учёбный центр «Информзащита», 12.01. 2004

[15] Beauregard J., Modeling information assurance, Air Force Institute of tehnology, 2001

Prof. dr LAZAR D. PETROVIĆ, dipl. el. inž.
Kriminalističko – policijska akademija, Beograd

Oblasti interesovanja: zaštita informacija, tehnologije zaštite informacionih sistema