Prof. dr Lazar Petrović, dipl. el. inž.
Udruženje sudskih veštaka za informacione tehnologije
IT VEŠTAK
Danijelova 32 Beograd
E – mail: lazar.petrovic48@gmail.com

OKRUGLI STO

„DIGITALNA FORENZIKA I IT VEŠTAČENJE U FUNKCIJI BORBE PROTIV VISOKO TEHNOLOŠKOG KRIMINALA“

INFORMACIONA BEZBEDNOST U SAVREMENOM SVETU

Gospodine predsedavajući, uvažene koleginice i kolege,

Dozvolite mi da se na početku zahvalim organizatorima ovog okruglog stola, Udruženju sudskih veštaka za informacione tehnologije - **IT VEŠTAK** iz dva razloga:

Prvo, zato što su ovu veoma interesantnu, ozbiljnu i nadasve aktuelnu temu savremenog društva stavili na dnevni red ovog skupa, i drugo, što su me pozvali da prisustvujem ovom skupu i dam svoj skromni doprinos u rešavanju ove veoma složene problematike.

Na početku treba reći da kod nas u Srbiji, problematika informacione bezbednosti nije do sada dovoljno razmatrana i nije joj posvećivana dovoljna pažnja. Jedan od razloga je svakako i nedovoljno poznavanje ove problematike u široj javnosti, a sa druge strane brz razvoj raznih elektronskih sistema u svetu i kod nas, što svakako usložnjava ovu multidisciplinarnu oblast. Otuda je pokretanje edukacije u ovoj oblasti, makar i preko ovako organizovanih okruglih stolova, za svaku pohvalu.

Da je tema informacione bezbednosti aktuelna pokazuju i najnovija zbivanja u svetu objavljivanjem poverljivih diplomatskih podataka na Internet sajtu Wikileaks koje je izazvalo opštu konfuziju u čitavom svetu. Međutim, ova tema je veoma kompleksna i njoj se može posvetiti čitava debata na nekom novom okruglom stolu, tako da je ovde samo spominjem kao interesantnu temu, koja može biti od interesa i za naše udruženje.

Kada govorimo o temi informacione bezbednosti treba, na početku, imati u vidu nekoliko činjenica.

U prvom redu treba se podsetiti nekih istorijskih činjenica koje su uslovile pojavu informacione bezbednosti. Istorijski posmatrano, prvo se pojavila 60 - ih godina prošlog veka, *komunikaciona bezbednost* (COMSEC – *communication security*). Sa pojavom kompjutera, 70 – ih godina, nastala je *kompjuterska bezbednost* (COMPUSEC – *computer security*), da bi se krajem 80 – ih godina COMSEC i COMPUSEC 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. Ovde treba istaći da

mnogi informatičari u startu imaju "sistemsku grešku" u poimanju informacionog sistema jer ga poistovećuju sa kompjuterskim sistemom. Izuzetno je važno shvatiti i prihvatiti sledeće činjenice:

1. Informacioni sistem nije isto što i kompjuterski sistem (Informacioni sistem ≠ Kompjuterski sistem)
2. Kompjuterski sistem je podsistem ili podskup informacionog sistema.

Da ne bude zabune evo nekoliko napomena: informacioni sistem pored kopmpjuterskog sistema čine i papiri s podacima u registratorima na policama arhive, telefaks uređaji i kopije faksova, telefonske mreže, video i ostali oblici nadzora, zaposleni i poslovni partneri (odnosno ono što oni znaju o podacima), fizička zaštićenost objekata, itd, itd. Očito da je pojam zaštite informacionog sistema izuzetno širok i kompleksan i prelazi poimanje informatičara koji to svode u pravilu samo na kompjuterski sistem. Ali, u krajnjem slučaju nije cilj zaštita samog informacionog sistema, nego onoga što se kao osnovna vrednosna jedinica nalazi u informacionom sistemu, a to je *informacija*. To znači da treba tako postaviti i organizovati informacioni sistem i sveukupne aktivnosti oko njega da ne dođe do nekontroliranog odliva ili promene sadržaja informacija koje se čuvaju i/ili obrađuju u informacionom sistemu. Iz tih razloga je INFOSEC osnovni akcenat stavio na sprečavanju *neautorizovanog* pristupa svim elementima informacionih sistema: izvoru informacija[1], sistemima za prenos, obradu i čuvanje svih vrsta informacija, i to pre svega, na poverljivost (*confidentiality*), integritet (*integrity*) i raspoloživost (*availability*) informacija.

Ovoj složenoj problematici **Informacione bezbednosti** pokušaću da pristupim sa dva aspekta, shodno zvanjima koja se nalaze u potpisu mog imena.

Prvo, u skladu sa mojim nastavnim zvanjem, rekao bih nešto o problematici školovanja kadrova u ovoj oblasti, kako za potrebe državnih tako i za potrebe privatnih organizacija. Počeo bih od pojmovnog određenja pojma *informacione bezbednosti*. Čini mi se da se pod pojmom **informacija**, usudio bih se reći, i u našim akademskim okvirima i stručnoj praksi, često smatra da su to samo podaci, poruke, saopštenja koja dolaze iz te jedne moćne mašine koju smo nazvali računarom ili kompjuterom. Međutim, prema teoriji informacija, koja se inače izučava na mnogim tehničkim fakultetima (prvenstveno elektrotehničkim), pojam informacije je daleko širi i obuhvata govorne, pisane informacije, informacije koje nosi pokretna ili nepokretna slika i niz drugih informacija, koje se mogu naći u nekom složenom sistemu, a služe za daljinski nadzor ili upravljanje, kako je napred istaknuto.

Podsetio bih da pojam *informacija* potiče od latinske reči *informare* koja znači: dati oblik, oblikovati, predočiti, predstaviti, odnosno uputstvo, obaveštenje, saopštenje, podatak o nečemu. Sa tehničkog aspekta *informacija* se definiše kao mera neizvesnosti nastajanja nekog događaja ili pojave. Ovo sam samo napomenuo da bismo pojmovno isto razmišljali o kakvim pojavama je reč, tako da bi je u razmatranjima tretirali na isti način.

A sada da se vratim pitanju **obrazovanja kadrova** u oblasti informacione bezbednosti.

Informaciona bezbednost, zbog svojih specifičnosti zahteva i posebno obrazovanje kadrova za rad u toj oblasti. To podrazumeva multidisciplinarni pristup, kako u sferi istraživanja tako i u oblasti obrazovanja. Zbog takve njene prirode, obučenost u sferi informacione bezbednosti podrazumeva usvajanje određenog fonda tehničkih, upravljačkih i specijalističkih znanja, tj. znanja koja se neposredno odnose na problematiku informacione bezbednosti. To znači da specijalista za

[1] Pod **izvorom informacija** treba podrazumevati elemente informacionog sistema gde nastaju razne vrste informacija: govor, pisane poruke, nepokretna i pokretna slika, podaci daljinskog merenja (telemetrijski podaci), podaci daljinskog upravljanja (teleupravljajući podaci), a ne samo informacije koje se javljaju u računarskim sistemima, bez obzira na njihov izvorni oblik (analogni ili digitalni oblik).

informacionu bezbednost mora posedovati, ne samo tehnička, već i upravljačka (menadžment, ekonomija, privredno pravo) i druga specijalistička znanja (organizacija sistema informacione bezbednosti, zaštita poslovnih tajni, specijalna psihologija, osnovi kriminalistike i industrijska špijunaža, itd.). Ovako definisani profil podrazumeva koordinaciju i konsultaciju sa nizom različitih sektora, koji međusobno mogu biti i prilično udaljeni, i fizički i organizaciono (finansijski, komercijalni, sektor proizvodnje, sektor informacionih tehnologija itd.). Očigledno je da stručnjaka ovakvog profila obično nema, ili ih je malo, tako da pojednine institucije moraju da rade na njihovom stvaranju.

Polazeći od toga da je informaciona bezbednost nov, složen i interdisciplinaran pojam, ona je predmet kako *tehničko - tehnoloških* naučnih istraživanja u oblasti informatike, elektromagnetike, obrade signala, itd., tako i *humaniratnih* naučnih istraživanja u oblasti sociologije, psihologije, prava, politologije, itd. Zbog ovakve njene prirode, obučenost u sferi informacione bezbednosti podrazumeva određeni fond tehničkih, upravljačkih i specijalističkih znanja, tj. znanja koja se neposredno odnose na problematiku informacione bezbednosti.

Obrazovanje stručnjaka za informacionu bezbednost se može izvoditi: na univerzitetetima, u specijalizovanim nastavnim centrima i u centrima na nivou ustanova za potrebe korisnika i osoba koje u njima rade.

Univerzitetsko obrazovanje pruža fundamentalna znanja, ali dugo traje. Inače, budućnost zahteva osmišljenu koncepciju univerzitetskog obrazovanja u oblasti informacione bezbednosti, što sada nije slučaj, prvenstveno na našim državnim fakultetima, mada to treba da bude primat i na nekim specijalističkim fakultetima i to prvenstveno na onim visokoškolskim ustanovama koji školuju kadrove za rad u državnim institucijama.

Kada je reč o nastavnim centrima, oni mogu biti: **nastavni centri kompanija** - prizvođača opreme za informacionu bezbednost i **specijalizovani nastavni centri** za pružanje usluga u sferi informacione bezbednosti obrazovanja.

Obrazovanje u centrima kompanija – proizvođača opreme je organizovano u vidu tematskih kurseva u trajanju od nekoliko dana do nekoliko nedelja u, od strane njih, interno autorizovanim centrima. Sadržaj kurseva je ili opšti ili se, što je češće, odnosi na konkretan proizvod i pravila njegove eksploatacije.

Specijalizovani nastavni centri organizuju tematski usmerene kurseve, sa teoretskim časovima i praktičnim laboratorijskim vežbama. Osim kompanijama, pripremu specijalista za informacionu bezbednost pružaju i državnim organizacijama.

Postoji i kombinovani pristup, koji objedinjava prednosti oba ova sistema.

Informaciona bezbednost u SAD

O značaju koji se pridaje informacionoj bezbednosti u **Sjedinjenim američkim državama** svedoči struktura upravljanja bezbednošću informacione infrastrukture. 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 analize informacija ISAC i Centar zaštite informacione infrastrukture federalnih agencija i ministarstava).

Zaštita informacione infrastrukture je predmet živog interesovanja u SAD. Tako npr. Insitut za zaštitu informacione infrastrukture[2] (čine ga 23 državne organizacije), na osnovu opsežnih ispitivanja, izdao je listu prioritetnih istraživanja u ovoj oblasti.

[2] I^3P – *Insitut Information Infrastructure Protection*

Pored čisto naučnih institucija, problematikom informacione bezbednosti se bave i neke druge institucije koje objedinjavaju teorijska 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 biltenima.

Naučno - istraživačka delatnost u ovoj oblasti definisana je sa prvih pet programa *Nacionalnog plana zaštite informacione infrastrukture* (iz 2000. godine) i pet nacionalnih prioriteta u oblasti zaštite informacione infrastruktura defisanih *Nacionalnom strategijom bezbednosti kiber prostora* (iz 2003. godine).

Svi američki univerziteti, počev od Univerziteta nacionalne odbrane UND, u svom sastavu imaju fakultete informacione bezbednosti.

Detalji koncepcije univerziteskog obrazovanja u SAD nisu mi poznati, ali mi je poznata ocelokupna organizacija problematike informacione bezbednosti, na državnom nivou.

Kada je reč o informacionoj bezbednosti u SAD, treba reći da postoji tesna saradnja državnog i privatnog sektora, što je definisano i u svim doktrinarnim dokumentima. O značaju koji se pridaje informacionoj bezbednosti u SAD svedoči struktura upravljanja bezbednošću informacione infrastrukture.

Pored čisto naučnih institucija, problematikom informacione bezbednosti se bave i neke druge institucije koje objedinjavaju teorijska i praktična istraživanja. Ove institucije prikupljaju statističke podatke o napadima i ranjivostima hardvera i softvera, pronalaze efikasne odgovore za protivdejstva i publikuju ih u biltenima.

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

Informaciona bezbednost u Ruskoj federaciji

Razmatranje pojma informacione bezbednosti (*информационноя безопасностъ*) **u Ruskoj federaciji** je novijeg datuma (od 90 - ih godina). Prema nekim analizama, bivši SSSR je izgubio hladni rat zbog zanemarivanja bezbednosti u informacionoj sferi društva.

Informaciona bezbednost 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),* odnosno, kao *stanje zaštićenosti informacione sredine društva koje omogućava njeno formiranje, korišćenje i razvoj u interesu građana, organizacija i države*. Kao polazno stanovište pri definisanju pojma uzet je interdisciplinarni pristup, tj. opšta nauka o bezbednosti. Uočava se, 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.

Korenite promene državne politike Ruskoj federaciji u oblasti nacionalne bezbednosti, odnosno informacione bezbednosti kao jedne od njenih osnovnih komponenti, dovela je do izrade koncepcije pripreme kadrova u oblasti informacione bezbednosti. Ova k*oncepcija* definiše osnovne zadatke, principe i pravce usavršavanja i formira metodološku osnovu za usaglašavanje aktivnosti svih subjekata zakonodavne i izvršne vlasti, obrazovnih institucija, naučnih organizacija, državnih i društvenih zajednica koje deluju o razmatranoj oblasti. Koncepcija proističe iz osnovnih zakonodavnih dokumenata Ruske federacije a, pre svega, iz Doktrine informacione bezbednosti po kojoj *nacionalna bezbednost Ruske federacije na suštinski način zavisi od obezbeđenja informacione bezbednosti*. Zbog toga je i profesionalna priprema, preobuka i usavršavanje kadrova

za informacionu bezbednost jedna od najvažnijih komponenti u kompleksu mera protivdejstava pretnjama, životno važnim interesima države u informacionoj sferi.

Znači, takvom koncepcijom je, u skladu sa doktrinom informacione bezbednosti Ruske federacije, problem informacione bezbednosti prestao da bude kompetencija specijalnih državnih službi, već je postao predmet interesovanja celog društva i građana.

Koncepciji pripreme kadrova za informacionu bezbednost je prethodio rad Državnog komiteta višeg obrazovanja (formiran 1992. godine) koji je između ostalog došao do zaključaka da je potrebno formirati funkcionalan sistem obrazovanja, da informaciona bezbednost ne može da se svede na tradicionalni pojam zaštite informacija, da je potrebno angažovanje širih društvenih i državnih struktura, a ne samo specijalista za informacionu bezbednost, da se obrazovanje ne može izvoditi van konteksta zakonodavno - pravnog regulisanja procesa informatizacije i da je neophodno da se na naučnoj osnovi zasnuje priprema, prekvalifikacija i usavršavanje kadrova za informacionu bezbednost.

U skladu sa navedenim zaključcima definisana je Koncepcija pripreme kadrova za informacionu bezbednost, a u cilju njene realizacije ukazom ministra obrazovanja Ruske federacije broj N 670 od 25. 02. 2003. godine, formiran je Koordinacioni savet ministarstva obrazovanja o problemima pripreme kadrova u oblasti zaštite državne tajne i informacione bezbednosti, formirana je grupa specijalnosti 075000 "Informaciona bezbednost", razrađeni su standardi višeg profesionalnog obrazovanja, nastavni planovi i programi kao i zahtevi za nastavno - metodičko i materijalno - tehničko obezbeđenje. U okviru istih nastojanja definisana je federalna komponenta informacione bezbednosti, programi usavršavanja i poslediplomske studije specijalnosti 05.13.19 "Metode i sistemi zaštite informacija. Informaciona bezbednost", sa 9 magistarskih i 12 doktorskih saveta.

U Ruskoj federaciji, danas se problematika bezbednosti i zaštita informacija (tzv. informaciona bezbednost), izučava na 148 raznih fakulteta. Pored ovoga, treba istaći da se obrazovanjem kadrova u oblasti informacione bezbednosti bave 12 ministarstava i ureda, mnoge naučne organizacije i institucije među kojima su i Moskovski državni institut Lomonosov i Akademija kriptografije Ruske federacije, da postoji 25 regionalnih nastavno - naučnih centara za probleme informacione bezbednosti i da postoje različiti kursevi za prekvalifikaciju i usavršavanje.

Analizom specijalnosi za informacionu bezbednost može se primetiti da u pregledu tih specijalnosti nedostaju one koje su vezane za humanitarne probleme: pravne, psihološke i socijalne. U tim analizama se ističe da će ovo biti jedan od prioriteta u budućem radu na problematici informacione bezbednosti. U ovom trenutku na fakultete za informacionu bezbednost se upusuje preko 5000 polaznika godišnje, sa tendencijom stalnog rasta broja upisanih studenata.

Kada su u pitanju *kursevi informacione bezbednosti u Ruskoj federaciji* situacija je sledeća. Postojeći kursevi su međusobno nezavisni jedan od drugog, bilo da se radi o kursevima u ruskim centrima, centrima autorizovanim od strane zapadnih kompanija, ili u nekim drugim insitucijama. Na kursevima se razmatraju neke konkretne teme, pri čemu se zaboravljaju ostali aspekte informacione bezbednosti. S druge strane, oni su pre svega teorijski, sa malo praktične obuke. Princip obuke koji je karakterističan za zapadnu metodiku obuke, a predstavlja postupnost u obuci, nije zastupljen na kursevima u Ruskoj federaciji. Pored nastavnih centara, autorizovanih od starne zapadnih firmi, u Ruskoj federaciji se pojavljuju i centri domaćih firmi (npr. "Информащита") koji organizuju kurseve ruskim firmama i ustanovama, u skladu sa realnim potrebama.

U Srbiji, koliko je meni poznato, problematika informacione bezbednosti nije, kao takva, dovoljno razmatrana. Pod terminima "*zaštita informacija*", "*bezbednost i zaštita informacija*" ili "*zaštita podataka*", "*protivelektronska zaštita*" tretirani su samo neki od aspekata informacione bezbednosti, uglavnom sa istorijski prevaziđenih stanovišta.

Činjenica da je, prema savremenim shvatanjima pojma nacionalne bezbednosti, informaciona bezbednost kao jedna od njenih osnovnih komponenti, problematiku informacione bezbednosti čini krajnje aktuelnom.

U Srbiji se na nekoliko fakulteta takođe izučava problematika bezbednosti i zaštite informacija. U Beogradu, koliko je meni poznato, pod nazivom "Bezbednost i zaštita informacija" ova oblast se izučava na Fakultetu bezbednosti, na Akademiji za diplomatiju i bezbednost, Kriminalističko – policijskoj akademiji, Vojnoj akademiji, mada se kadrovi za rad u državnim organima školuju i na nekoliko namenskih visokoškolskih institucija.

Cilj izučavanja ovakvog predmeta bi trebao da bude da studente upozna sa raznim aspektima ugrožavanja i zaštite informacija kao i sa važećom zakonskom regulativom i standardima u ovoj oblasti. Studenti treba da se upoznaju sa osnovnim pojmovima iz oblasti zaštite poslovnih (službenih) tajni kao i sa zaštitom od industrijske špijunaže. Nastavni sadržaji koji bi se izučavali kroz ovakav predmet, treba, pored ostalog, da obuhvate sigurnost i zaštitu informacija kroz sve aspekte zaštite, kako organizacione tako i tehničke aspekte zaštite i to svih vrsta informacija.

Zaštita informacija, koliko je važna za civilne strukture bezbednosti, još je važnija za državne bezbednosne strukture, pa joj se u tim strukturama mora dati poseban značaj.

Kada je reč o problematici informacione bezbednosti u Republici Srbiji, treba reći i to, da u Srbiji ne postoji ni jedno mesto gde se izvode kursevi obuke u oblasti informacione bezbednosti.

Potvrda o kvalitetu izvedene obuke se iskazuje sertifikatom. Postoje dve različite šeme za dobijanje sertifikata, u skladu sa definisanim načinom obučavanja. Koliko je meni poznato ni Ruska federacija ni Srbija nemaju svoje sertifikate. Takođe nije mi poznato ni da u Republici Srbiji postoje, autorizovani centri za polaganje i dobijanje takvih sertifikata. U dostupnoj literaturi se čak i ne pominje da je iko iz ovih krajeva stekao neki od navedenih sertifikata.

Drugo, kao inženjer elektrotehnike, elektronike i telekomunikacija, po osnovnom obrazovanju, koji se duži niz godina bavi problematikom elektromagnetnih zračenja, koja je kod nas nedovoljno tretirana, rekao bih nešto i o uticaju tog zračenja na bezbednost informacija, odnosno pokušaću da toj problematici pristupim sa jednog čisto tehničkog aspekta.

Da bi se shvatilo i razumelo pitanje elektromagnetnog zračenja potrebno je definisati neke osnovne pojmove. Kao prvo, potrebno je definisati pojam **elektromagnetnog zračenja** (EMZ). Pod tim pojamom podrazumeva se emitovanje elektromagnetne energije određene talasne dužine, odnosno na određenoj frekvenciji. Ova pojava, sama po sebi ima, kako korisne tako i štetne efekte. Korisni efekti se višestruko koriste u mnogim oblastima savremene civilizacije, za opštu dobrobit čovečanstva. Međutim, kako to obično biva u prirodi, prateći štetni efekti se veoma često, zbog različitih razloga zaboravljaju, iako su stručnjacima poznati. Ti efekti se, ponekad mogu zloupotrebiti i staviti u funkciju protiv čoveka, odnosno mogu se upotrebiti kao oružje koje izaziva poremećaje u radu pojedinih savremenih elektronskih uređaja i sistema, pa čak i kao oružje za fizičko uništenje raznih živih bića i čoveka.

Odavno je poznato da se radiološko ili tzv. jonizirajuće zračenje pojedinih radioaktivnih materijala može koristiti kao nekonvencionalno oružje, napravljeno u vidu atomske bombe, što je, na žalost, krajem Drugog svetskog rata i isprobano u japanskim gradovima Hirošima i Nagasaki. O prirodi i efektima ove vrste oružja je dosta napisano i postoji brojna svetska i domaća literatura, tako da ovde neće biti govora o ovoj vrsti zračenja.

Drugu grupu elektromagnetnih zračenja čine tzv. nejonizirajuća zračenja. Tu spadaju: ultravioletno (UV) zračenje (talasnih dužina 100 – 400 nm[3]), vidljivo svetlosno zračenje (400 – 780 nm), infracrveno (IC) zračenje (780 nm – 1 mm), radiofrekventno (RF) zračenje (100 KHz – 300 GHz, u

[3] nm – nanometar ($1nm = 10^{-9}$ m)

koje se ubrajaju i mikrotalasno zračenje od 300 MHz do 300 GHz), promenljiva električna i magnetska polja i lasersko zračenje.

Svako elektronsko sredstvo je tokom eksploatacije izloženo raznovrsnim elektromagnetskim efektima. Sa druge strane ono tokom rada generiše elektromagnetnu energiju i vrši uticaj na druga sredstva u svom okruženju. Da bi se ograničio ovaj međusobni uticaj propisuju se standari kojima se regulišu dozvoljeni nivoi zračenja, odnosno definiše se osetljivost pojedinih sredstava na elektromagnetna zračenja. Pored ovih opasnosti koje postoje pri radu elektronskih sredstava (prvenstveno telekomunikacionih i računarskih sredstava), postoji i opasnost oticanja sadržaja podataka (informacija) koji se obrađuju u konkretnom sredstvu i/ili se prenose preko telekomunikacionih sistema. Ovo je posebno aktuelno i opasno u funkcionalnim telekomunikacionim i računarskim sistemima gde postoji potreba da se tim sistemima, često puta, prenose i obrađuju podaci i informacije poverljive prirode.

Problematika EMZ se zasniva na dva osnovna zakona fizike:

1. Kada električna struja protiče kroz neki provodnik ona generiše elektromagnetnu energiju u vidu elektromagnetnog talasa.
2. Promenljivi elektromagnetni talas generiše (indukuje) električnu struju u bilo kojoj provodnoj strukturi koja se nađe na njegovom putu.

Znači, kada električna struja protiče kroz neki provodnik ona generiše elektromagnetnu energiju u vidu elektromagnetnog talasa. Ovaj talas se prostire brzinom svetlosti kroz okolinu, i obrnuto, tj. promenljivi elektromagnetni talas generiše (indukuje) električnu struju u bilo kojoj provodnoj strukturi koja se nađe na njegovom putu. Nivo indukovane elektromotorne sile zavisi od amplitude elektromagnetnog talasa koji je uzrokuje. Tako, električni i elektronski sistemi, svi računari i telekomunikaciona oprema i svi metalni kablovi kojima se oni spajaju, zrače elektromagnetnu energiju, na opisani način i u merljivim iznosima.

Elektromagnetna energija se od izvora do prijemnog uređaja može prenositi **vođenjem**, kada su izvor i prijemnik direktno spojeni vodovima ili vodljivim pločama, ali isto tako električnom ili magnetnom spregom, na manjim udaljenostima, ili **zračenjem** na većim udaljenostima. Dobro poznavanje pojave u elektromagnetnim sistemima i veze između korisnih i parazitnih signala važno je, ne samo za ispravan rad pojedinih vrsta uređaja nego je često od prvorazrednog značaja za tajnost poruka u telekomunikacionim ili računarskim sistemima.

Za radiokomunikacione sisteme je jasno da se poruke koje se predaju pomoću elektromagnetnih talasa mogu primati i na velikim udaljenostima, pa se unapred pre predaje provode mere u svrhu zaštite tajnosti tih poruka. Kod računarskih sistema, a posebno terminala (klasičnih ili inteligentnih), nisu preduzete nikakve mere zaštite, osim u izuzetnim slučajevima, pa se lako mogu primati poruke i to najčešće preko parazitnih elektromagnetnih signala.

Proučavanje elektromagnetnih pojava u elektronskim sistemima koje se dešavaju na korisnim i parazitnim frekvencijama, kao i postupaka koji osiguravaju elektromagnetsku kompatibilnost mogu vrlo dobro poslužiti i za provođenje mera zaštite tajnosti poruka, bilo u fazi dok se uređaji i sistemi projektuju i proizvode ili na već gotovim uređajima i sistemima.

Prema tome, svi uređaji koji koriste EM energiju neminovno uz energiju na željenim frekvencijama generišu i signale na neželjenim frekvencijama. Signali na neželjenim frekvencijama javljaju se kao elektromagnetne smetnje, i svojim prisustvom i nivoima mogu ugroziti rad drugih uređaja u svojoj okolini, i sa druge strane, u generisanim neželjenim signalima može biti sadržan podatak o informaciji koja se prenosi, što često puta predstavlja poslovnu, vojnu ili drugu vrstu tajni.

Kada elektronsko sredstvo (telekomunikaciona oprema, elektronski računar i drugo elektronsko sredstvo) radi u nekom svom okruženju ono je izloženo raznovrsnim elektromagnetnim (EM) efektima, a takođe i ono generiše uticaje takve vrste. Ovi efekti se opisuju kao EM uticaj, odnosno EM

zračenje. Za svako elektronsko sredstvo je važno znati koji nivo EM zračenja ono može izdržati, a takođe i koji nivo EM zračenja ono proizvodi tokom normalnog rada. Podaci o nivoima ovih zračenja su važni kod projektovanja opreme i definisanja stepena zaštite od raznovrsnih uticaja. Za ispravno i normalno funkcionisanje elektronske opreme važno je poznavanje dejstva oba navedena uticaja. Zbog toga je podatak o nivou EM zračenja veoma važan i govori o značaju koji se mora pokloniti sistemima i njihovom okruženju.

Tehnički problemi koji se javljaju u vezi sa EM zračenjem mogu se posmatrati kroz nekoliko jasno izraženih pojava kao što su:

1. Pojava **elektromagnetnih smetnji (EMS)** koje ugrožavaju kompatibilnost posmatranog elektronskog sredstva u neposrednom okruženju;
2. Pojava **elektromagnetnih zračenja (EMZ)** koja su štetna po zdravlje ljudi (posebno zračenja u mikrotalasnom spektru) i
3. Pojava **parazitnih (informacionih) elektromagnetnih zračenja (PEMZ)** preko kojih neželjeno mogu oticati informacije koje se prenose i obrađuju u uređajima i/ili sistemima.

Elektromagnetne smetnje EMS (EMI – **E**lectro **M**agnetic **I**nterference) su ometajući signali ili šumovi koji utiču na korektnost funkcionisanja električnih i elektronskih uređaja. Dejstvo ovih smetnji, poznatih i pod nazivom radiofrekventne smetnje RFS (RFI – **R**adio **F**requency **I**nterference), oseća se u celoj sredini u kojoj su prisutne. Njihovo delovanje kreće se od smanjenja kvaliteta veza u telekomunikacionim sistemima (radio i TV sistemima) do mogućnosti ometanja pojedinih elektronskih uređaja i sistema koji se koriste u različitim oblastima ljudske delatnosti (istraživanjima, medicini i drugo).

Problem sve većeg prisustva smetnji u svim sredinama, komplikuje se činjenicom da su tehnički sve složeniji savremeni elektronski sistemi istovremeno i sve osetljiviji na uticaj elektromagnetnih smetnji.

Elektromagnetna energija ima takvo svojstvo da se može prostirati kako preko vodova tako i putem zračenja u slobodnom prostoru. Zračenje elektromagnetne energije na neželjenim frekvencijama predstavlja pojavu elektromagnetnih smetnji. To znači da svi uređaji tokom rada zagađuju okolinu zračenjem elektromagnetne energije. Elekromagnetno zagađenje okoline adekvatno je ostalim zagađenjima životne sredine, pa bi takav tretman trebalo i da ima pri rešavanju tih problema. Ovo zračenje može biti uzrok pojavi smetnji u radu drugih osetljivih elektronskih uređaja, tim pre što nivo zračenih signala može biti znatno viši od praga osetljivosti prijemnika. Zbog mogućnosti međusobnog uticaja, danas se u svetu posvećuje sve veća pažnja racionalnom korišćenju ukupnog elektromagnetnog spektra.

Problem rada uređaja u prisustvu elektromagnetnih smetnji definiše se kao **elektromagnetna kompatibilnost** (EMK). To je sposobnost jednog elektronskog, električnog ili elektromehaničkog uređaja ili sistema da radi u radnoj okolini tako da ne izazove nedozvoljenu degradaciju u funkciji drugih uređaja ili sistema ili da sam ne bude ometan do te mere da se poremeti njegova osnovna funkcija, odnosno sposobnost uređaja ili sistema da funkcioniše na zadovoljavajući način u svom elektromagnetnom okruženju, ne prouzrokujući pri tom sopstveni elektromagnetni uticaj na susednu opremu, instrumente ili sisteme. Problem elektromagnetne kompatibilnosti se nekada rešavao u trenutku kada je dolazilo do međusobnog delovanja pojedinih uređaja ili sistema, odnosno kada je rad jednog uređaja izazivao smetnje u radu drugog uređaja. Iz tih razloga se ponekad, a pogotovu u funkcionalnim sistemima, postavljaju veoma strogi zahtevi u pogledu ostvarivanja visokog stepena elektromagnetne kompatibilnosti.

Pravilan način kojim se osigurva visoki stepen elektromagnetne kompatibilnosti i racionalno iskorišćenje elektromagnetnog spektra jeste iznalaženje mogućnosti predviđanja situacija koje

mogu nastupiti. To zahteva proučavanje i poznavanje izvora elektromagnetnih smetnji, načina nastanka i prenosa tih smetnji i prijemnika koji prima ove smetnje.

Izvori elektromagnetnih smetnji su mnogobrojni i pokrivaju veoma širok frekventni opseg.

Prirodni izvori elektromagnetnih smetnji, EMI, su munja i druge atmosferske smetnje, promene u zemljinom magnetnom polju, jonosferske promene, itd.

Veštački izvori mogu biti namerno izazvana zračenja, kao što je slučaj kod radio, televizijskih i radarskih predajnika, nuklearne eksplozije i slično, ili mogu nastati neželjeno, kao posledica samih karakteristika uređaja ili kvara na uređaju. U osnovi, sva elektronska kola mogu emitovati smetnje različitog intenziteta i frekvencije.

Pojava EM smetnji obuhvata dve vrste smetnji i to: izračene elektromagnetne smetnje (polje EMS) i konduktivne elektromagnetne smetnje. Nivoi ovih EMS definišu se posebnim međunarodnim i nacionalnim standardima (IEC, MIL, JUS, SNO i dr.).

Druga pojava je **pojava štetnog delovanja elektromagnetnih zračenja na žive organizme**. Što se tiče pojave štetnog delovanja po zdravlje ljudi, treba reći da se tu javljaju termički i elektrohemijski efekti koji dovode do stvaranja električnih struja u organizmu, kao i neki drugi efekti, izazvani električnim i magnetnim poljem nastalog od radiofrekventnog zračenja.

Osnovni vid dejstva RF zračenja je termički (toplotni efekat) koji dovode do zagrevanja tkiva, mada se javljaju i drugi – netermički efekti.

Kod lokalnog izlaganja RF zračenju visokih intenziteta može doći do opekotina na koži i u mišićima, a kod izlaganja očiju do zamućenja sočiva. Na lokalno zagrevanje RF zračenjem takođe su veoma osetljivi polni organi čoveka. Takođe može doći do promena u ponašanju, promene u centralnom nervnom sistemu, krvotoku i odbrambenom sistemu (što se može i zloupotrebiti). Nije dokazano da dugotrajno izlaganje RF zračenju niskog intenziteta dovodi do značajnijeg oštećenja zdravlja, malignih oboljenja i posledica po potomstvo.

Promenljiva električna i magnetna polja ekstremno niskih frekvencija, koja većinom nastaju od toka naizmenične struje, najčešće frekvencije 50 Hz, izazivaju pojavu indukovanih struja koje mogu uticati na rad srca, nervnog tkiva i drugih organa. Tim električnim i magnetnim poljima su najviše izloženi radnici zaposleni na održavanju dalekovoda, transformatora, električari i drugi radnici "električarskih" zanimanja, zavarivači, radnici na indukcionim pećima, na električnoj železnici, itd.

Biološko dejstvo oba polja se obično proučava odvojeno i smatra se da magnetno polje ima veće značenje. Električna i magnetna polja u telu čoveka izazivaju pojavu indukovanih struja, koje, ako su dovoljne gustine, mogu da utiču na prirodne struje u organizmu, odnosno na rad srca, nervnog tkiva i drugih organa. Postoji sumnja da ta polja imaju i druge efekte koji nisu, nažalost, u dovoljnoj meri proučeni. U svakom slučaju, treba izbegavati nepotrebno izlaganje tim poljima.

Zračenje televizijskog aparata, video terminala ili monitora PC računara nije preterano štetno po zdravlje njihovih korisnika, jer izmereni nivoi zračenja su veoma niski i nalaze se u dozvoljenim granicama, koje često ne prelaze one nivoe koji se nalaze u prirodnoj životnoj sredini.

Ovde treba istaći da je zračenje mobilnog telefona, zbog načina korišćenja, daleko opasnije od elektromagnetnih zračenja koja nastaju od drugih elektronskih sredstava. Iako su mobilni telefoni postali nezamenljivi u životu savremenog čoveka, čak toliko da mnogi ne mogu da zamisle život bez ovih uređaja, lekari upozoravaju da su mobilni telefoni opasni za nervni, ali i endokrini i reproduktivni sistem čoveka. Po mišljenju naučnika, opasnost se krije u tome što se biološki efekat elektromagnetnog polja akumulira tako da nastaju odložene posledice, među kojima su razvoj degenerativnih procesa centralnog nervnog sistema, ali i leukemija ili rak mozga, kao i hormonalna oboljenja. Elektromagnetni talasi su posebno opasni za decu i trudnice u odmakloj fazi trudnoće, zbog čega se budućim majkama savetuje da što je moguće više skrate razgovore mobilnim

telefonom, a u mnogim zemljama je deci ispod 14 godina zabranjena upotreba mobilnog telefona. Mnogobrojna istraživanja dokazuju da ljudski organizam reaguje na ova zračenja. Iako te reakcije još nisu u potpunosti proučene, niko ne osporava da je pri korišćenju mobilnih telefona neophodna odgovarajuća kultura. Eksperti ukazuju da su bezbedniji kratki razgovori, zbog čega savetuju da je bolje razgovarati pet puta po jedan minut, nego jednom pet minuta. Interval između poziva bi trebalo da bude najmanje petnaest minuta.

Nivoi dozvoljenog elektromagnetnog zračenja mogu se izražavati i preko definisanih zona dozvoljenog zračenja za koje su date dozvoljene površinske gustinu snage. Tako je *zona vrlo intenzivnog zračenja* sa površinskom gustinom većom od 10 mW/cm^2, *zona intenzivnog zračenja* 1 – 10 mW/cm^2 (15 min. u 24 sata), *zona umerenog zračenja* 0,1 – 0,9 mW/cm^2 (3 sata u 24 časa) i *zona slabog zračenja*, koje iznosi manje od 0,1 mW/cm^2.

Dozvoljeni nivo gustine snage elektromagnetnog zračenja je u mnogim zemljama regulisan nacionalnim standardima. Na primer, prema švedskom standardu taj nivo iznosi 450 $\mu W/cm^2$ (0,45 mW/cm^2), što odgovara jačini električnog polja E = 41 V/m. Naš, standard je mnogo strožiji tako da dozvoljeni nivo gustine snage elektromagnetnog zračenja iznosi 200 $\mu W/cm^2$, odnosno jačina električnog polja je E = 27,5 V/m.

Da bi se shvatilo koliki su iznosi navedenih nivoa gustine snage elektromagnetnog zračenja treba reći da nivo zračenja nebeskih tela (Sunce, zvezde) iznosi 14 pW/cm^2, a da taj nivo kod ljudskog tela iznosi oko 0,5 $\mu W/cm^2$.

Treći efekat elektromagnetnih zračenja, tj. pojava **parazitnih, informacionih elektromagnetnih zračenja** (PEMZ), se intenzivno izučava u svetu ali se rezultati tih istraživanja čuvaju u najvećoj tajnosti i javno se ne publikuju. Zahtevi za PEMZ se obično postavljaju na opremu koja se koristi u funkcionalnim sistemima, ali se sve više postavljaju ovi zahtevi i za opremu druge primene. Energija takvog zračenja je u direktnoj vezi sa podacima koji se obrađuju i prenose sistemima. Rezultujući EM talasi takvog zračenja mogu biti nosioci poverljivih podataka koji se mogu detektovati i analizirati, kako u lokalu, tako i sa određenog rastojanja. Ovi talasi mogu u originalnim podacima prouzrokovati greške, bilo superponiranjem sa drugim podacima ili brisanjem kompletnih podataka. To se koristi u oblasti tzv. "industrijske i druge špijunaže" kada se EM talasi, koji sadrže podatke nad kojima se obavlja neka obrada, mogu detektovati i zabeležiti pomoću vrlo osetljivih prijemnika. Zbog toga se nastoji izvršiti određena zaštita od ovih zračenja. Čak i kada se ovakvo zračenje ne može u potpunosti sprečiti, ono se, ipak, primenom određenih mera zaštite može u znatnoj meri smanjiti.

Iako su zahtevi za dozvoljene nivoe zračenja (EMS, EMZ, i PEMZ) međusobno različiti, blokiranjem jednog tipa smetnji, odnosno zračenja, blokiraju se, u određenoj meri, i ostala zračenja.

Podela neželjenog elektromagnetnog zračenja na EMS, EMZ i PEMZ izvršena je prema efektima koje konkretno zračenje može izazvati. S obzirom na područje koje ta zračenja zauzimaju u EM spektru, korektnije je reći da se radi o radio – frekvencijskim smetnjama (RFS). Ovako definisane RFS predstavljaju EM energiju koja izaziva neželjene posledice (ugrožavanje kompatibilnosti, štetnost po zdravlje, oticanje informacija). Sva tri efekta elektromagnetnog zračenja treba da budu predmet posebnog interesovanja, pa se po svim ovim temama mogu na sličan način organizovati okrugli stolovi, jer ti efekti direktno utiču na bezbednost kako osetljive elektronske opreme tako i na bezbednost obrađivanih i memorisanih podataka i informacija, kao i na bezbednost ljudstva koje rukuje takvim sredstvima.

U nastavku će uglavnom biti reči o trećoj pojavi tj. o opasnostima koje se javljaju zbog mogućnosti oticanja poverljivih podataka putem parazitnih elektromagnetnih zračenja i merama i postupcima kojima se to zračenje svodi u okvire koji ne predstavljaju realnu opasnost za kompromitaciju sadržaja informacija koje se obrađuju u računarskim i telekomunikacionim sistemima, tj. informaciona bezbednost.

Bezbednost podataka se može sagledati sa više aspekata. To su fizička bezbednost opreme, bezbednost primenjenog softvera i bezbednost primenjenog zaštitnog koda. Posebnu pažnju zaslužuje i aspekt zaštite opreme od tzv. "curenja" podataka. Ukoliko ova zaštita nije pravilno projektovana to ima za posledicu emisiju parazitnog zračenja iz opreme pre kodovanja, koja se može "uhvatiti" direktno, indirektno ili provođenjem. To su elektromagnetni gubici koji se mogu pokupiti i kao takvi upotrebiti, što predstavlja nelegalni pristup poverljivim informacijama.

Nivoi EM zračenja koji potiču od računara i telekomunikacionih sistema, čak iako veoma mali, još uvek su dovoljno visoki da bi se mogli detektovati tzv. “TEMPEST” prijemnicima (**T**otal **E**lectronic and **M**echanical **P**rotection against the **E**mission of **S**purious **T**ransmissions). TEMPEST predstavlja tehnologiju koja se odnosi na ograničavanje neželjenih elektromagnetnih zračenja prilikom obrade podataka u elektronskim uređajima i pokriva sve tehnike koje se koriste u borbi protiv industrijske i druge špijunaže. Zaštita od elektromagnetne špijunaže obuhvata proučavanje prirode izračenih podataka s ciljem da se proveri da li se oni mogu dovesti u vezu sa nekom poverljivom informacijom. Konačan cilj je da se ograniče mogućnosti neovlašćenog korisnika da prikuplja informacije o unutrašnjem protoku podataka unutar računara ili telekomunikacione opreme. Ako se prijemnik poveže sa dodatnom opremom onda se može vršiti analiza sadržaja signala, uz odgovarajuća upoređivanja sa referentnim signalom. Ukoliko se na ovakav način zaključi da dolazi do oticanja sadržaja poverljivih podataka, onda je potrebno izvršiti odgovarajuću zaštitu. Oprema kojom se vrše ovakva ispitivanja i analize je uglavnom programabilna, što pojednostavljuje proces ispitivanja, a ako se takva analiza vrši u špijunske svrhe to znači da se celokupan proces može i mora pratiti u realnom vremenu. Podaci o Tempest tehnologiji su poverljive prirode i u javnosti su nedostupni.

Zaštitne mere kojima se nastoji sprečiti ili umanjiti uticaj EM zračenja, u cilju povećanja bezbednosti podataka koji se obrađuju i prenose određenim sistemom, provode se na hardveru ili pomoću dodatnih hardverskih zahvata. Normalni postupak je definisanje različitih nivoa potrebne zaštite ili prihvatljivih nivoa osetljivosti za konkretnu opremu. To se obavlja još u fazi projektovanja opreme. Na nesreću, iz različitih razloga, ponekad iz tehničkih, a ponekad iz komercijalnih, ovaj postupak se, u mnogim slučajevima, primenjuje nedovoljno i neadekvatno.

Problemi u vezi bezbednosti podataka nastaju usled pojave industrijskog EM zračenja i, kao posledica toga, potreba za zaštitom od takvog zračenja. Bezbednost sistema (telekomunikacionih i računarskih) u kojima se vrši prenos i obrada informacija predstavlja pitanje stepena poverenja u podatke koji se prenose ili obrađuju u takvim sistemima. Bezbednost se može sagledati sa više različitih aspekata i to kao, fizička bezbednost opreme, bezbednost primenjenog softvera i bezbednost primenjenih kodova. Poseban aspekt u pogledu bezbednosti, koji zaslužuje pažnju je zaštita od oticanja podataka (“curenje “ podataka) koja, ako nije pravilno projektovana ima za posledicu emitovanje parazitnog zračenja, pre provođenja zaštitnog kodovanja. Ovo zračenje se može detektovati direktno ili indirektno, ili se može primati konduktivnim putem. Podaci do kojih se dolazi na ovaj način mogu biti nenamenski upotrebljeni, a to predstavlja nedozvoljeni pristup poverljivim informacijama. Za prijem, merenje i analizu podataka koje generiše, prenosi i obrađuje telekomunikaciona i računarska oprema koriste se specijalni, vrlo osetljivi merni prijemnici, tzv. “Tempest” prijemnici. Ovaj problem je jednako prisutan i u analognim i u digitalnim sistemima.

Pitanjima bezbednosti obrade informacije u kompjuterskim i telekomunikacionim sistemima za sada se u našoj zemlji bavi samo uski krug stručnjaka. To je, naravno, u velikoj meri uslovljeno našim zaostajanjem u primeni savremene tehnike. Ipak, život nas je sve stavio u takve uslove da je sveopšta digitalizacija i kompjuterizacija odavno prestala da bude inostrana egzotika i privilegija. To inspiriše, ali treba shvatiti da kompjuterizacija, osim očiglednih i široko reklamiranih koristi, sa sobom nosi, kao prvo, značajan utrošak napora i resursa, a kao drugo, mnogobrojne probleme razumljive još uvek samo uskom krugu ljudi.

Jedan od tih problema, pri čemu možda i jedan od najvećih, jeste problem obezbeđenja sigurne obrade poverljivih informacija u telekomunikacionim i kompjuterskim sistemima.

Do sada se ovaj problem više - manje ozbiljno pojavljivao samo u državnim, policijskim i vojnim službama, kao i u naučnim krugovima.

Najopasniji izvori **PEMZ**-a su displeji, kablovske linije veze, disk - memorija i teleprinteri serijskog tipa. Na primer, s displeja se informacija može skinuti pomoću specijalne aparature na rastojanju do 500 – 1500 m, s printera do 100 – 150 m. Presretanje PEMZ – a može se ostvarivati i pomoću prenosne (mobilne) opreme.

Ovde su nabrojani samo neki od mogućih kanala oticanja informacija. Dobijeni podaci mogu se koristiti na prvoj etapi stvaranja kompleksnog sistema zaštite informacija, tj. pri analizi pretnji oticanja poverljivih informacija.

U domenu zaštite informacija, posebno u određenim vrstama poslovanja, postoje zakoni, standardi, uredbe, instrukcije metodike i norme koje se dorađuju i preciziraju, polazeći od zahteva vremena, državne strukture i savremenog nivoa nauke i tehnike.

Pojam *poslovna tajna* koristi se da se označi informacija, dostupna ograničenom broju korisnika, koja nosi poverljivi karakter. Zaštita takve nformacije briga je samih korisnika, rukovodilaca i drugih komercijalnih struktura. Za zaštitu poverljive informacije ne postoje stroga zakonska pravila, zahtevi i norme, niti su postojeće nešto posebno poštovane, a oni koji su odavali poslovne tajne uglavnom su nikako ili samo uslovno zakonski sankcionisani.

Nažalost, mora se konstatovati činjenica da mnogi rukovodioci, ne poklanjaju pitanju zaštite informacija dovoljno pažnje i počinju da brinu tek kad se primeti oticanje informacije u ruke neovlašćenih lica.

Svi su već odavno shvatili da je na savremenom nivou razvoja društva informacija možda najskuplja roba. Po mišljenju stranih specijalista, pri potpunom otkrivanju svih informacionih sistema, samo 20% preduzeća srednje veličine opstalo bi još nekoliko sati, gotovo polovina - svega nekoliko dana, ostali - do nedelju dana. Ista sudbina zadesila bi i banke. Informacija je jedan od najvažnijih izvora blagostanja svake institucije. Ne kaže se uzalud: "*Ko poseduje informaciju, poseduje svet*". Svaka administrativna odluka zasniva se i vredi kao informacija na osnovu koje je doneta.

Osnovni preduslov za izgradnju svakog sistema zaštite je da se zna: ko ili šta štiti, od čega se štiti i kakve su moguće posledice ako se informacije ne štite. Sistem zaštite telekomunikacionih i računarskih sistema u mnogome zavisi od procene i analize opasnosti koje deluju na sistem. U svakom slučaju, cilj treba da bude kompletna zaštita sistema u toku obrade i prenosa informacija. Ukoliko nije zaštićena samo jedna komponenta, nelegalni korisnik može, koristeći tu komponentu, da prodre u sistem, pa činjenica da su svi ostali elementi dobro zaštićeni, gubi smisao. Treba imati u vidu da *mehanizam zaštite čini lanac koji je efikasan i siguran upravo onoliko koliko je jaka njegova najslabija karika*.

Imajući sve ovo u vidu, problem zaštite nebi smeo biti prepušten samo imaocima savremenih elektronskih sistema, njihovim improvizovanim dogovorima i parcijalnim rešenjima, jer on dobija takve razmere da prestaje biti samo njihov problem, već poprima karakter opštedruštvenog problema i postaje adekvatan drugim velikim problemima savremenog društva. Potvrda tome je i činjenica da je zaštita u računarima, računarskim i telekomunikacionim mrežama predmet studija, rasprava i odluka različitih nacionalnih i međunarodnih tela i organizacija, a broj zemalja koje su ovu materiju regulisale i zakonom, stalno se povećava.

Treba reći da postoje razni načini pojedinačne zaštite kojima se može, koliko toliko uticati na smanjenje nivoa elektromagnetnog zračenja.

Na kraju se može reći da su savremeni računarski i telekomunikacioni sistemi izuzetno složeni sistemi koji se ni u jednom trenutku ne smeju podceniti, jer opasnosti koje posredno ili neposredno ugrožavaju te sisteme toliko su međusobno povezane i isprepletane tako da nad celim sistemima formiraju krajnje kompleksnu mrežu opasnosti. U takvim sistemima bliski terminali se vezuju na

centralni računar ili pomoću koaksijalnih kablova ili u novije vreme optičkim provodnicima, zbog niza prednosti koje pružaju ovi sistemi prenosa. Udaljeni terminali povezuju se na centralni računar pomoću obične telefonske parice, koja je podložna raznim uticajima, pa se na prenosnom putu mora vršiti kriptološka zaštita sadržaja podataka.

Iz ovoga se može zaključiti da je u računarskoj mreži pitanje zaštite daleko složenije u odnosu na sisteme sa "lokalnom" obradom i centralizovanom terminalskom mrežom.

Sve ovo ukazuje na potrebu preduzimanja adekvatnih mera i akcija, ne gubeći iz vida realne mogućnosti i potrebe. Jer, iako svaki računarski sistem zahteva određeni sistem zaštite, oni su retko identični u pogledu svojih siguronosnih zahteva, koji u najvećoj meri zavise od vrste i veličine računarskog sistema, vrste, količine i značaja podataka i informacija, broja i strukture korisnika, kao i od nivoa automatizacije i kompleksnosti ukupnog informacionog sistema.

Sa stanovišta informacione bezbednosti, posebno je aktuelna i mogućnost dolaženja do sadržaja obrađivanih podataka u računarskim sistemima putem parazitnih elektromagnetnih zračenja. U vreme razvijene tehnike i moderne tehnologije, ovo predstavlja realnu opasnost na koju se, pogotovu u funkcionalnim računarskim sistemima, mora obratiti posebna pažnja.

Problem parazitnih elektromagnetnih zračenja je veoma složen jer je frekventni spektar zračenja veoma širok pa tehnologije koje se primenjuju i efikasne su za jedan deo opsega nisu uvek efikasne u drugom delu frekventnog spektra.

Neosporno je da se putem parazitnih elektromagnetnih zračenja mogu "hvatati" i obrađivati informacije koje se obrađuju u računarima i to kako sa bliskih tako i sa većih udaljenosti. Smatra se da se loše zaštićeni sistemi mogu efikasno pratiti čak i sa udaljenosti od jednog kilometra od uređaja.

Zaštitom od parazitnih elektromagnetnih zračenja, (TEMPEST), rešava se i pitanje elektromagnetne interferencije, EMI, tj. uticaj računara na ostale elektronske uređaje u njegovoj blizini i uticaj drugih uređaja na računar.

Zaštita od neželjenih parazitnih elektromagnetnih zračenja predstavlja relativan pojam, jer je skoro nemoguće sva neželjena zračenja svesti na nulti nivo. Nekada je dovoljno obezbediti takvu zaštitu da se spreči prijem signala parazitnih zračenja na udaljenostima od 1 km, a ukoliko bi neovlašćeni korisnik ipak želeo doći do podataka koji se obrađuju u računaru onda se mora približiti sa kompletnom kompleksnom mernom opremom, a to se onda rešava na drugi način i drugim metodama zaštite.

Pokušao sam da kroz ova dva pitanja ukažem na ozbiljnost celokupne problematike informacione bezbednosti. Smatram da je na ovom okruglom stolu samo iniciran veoma obiman i složen problem informacione bezbednosti, što je u svakom slučaju za pohvalu. Predlažem da se sa ovog, a i kasnijih okruglih stolova, donesu konkretni zaključci sa kojima treba upoznati relevantne državne institucije, kako bi se ovako važna pitanja počela rešavati na državnom nivou.