KEMZ I INFORMACIONA BEZBEDNOST

Milorad S. Markagić, Vojna Akademija, e-mail: milmarkag@yahoo.com

Izvod: *Cilj ovog rada je da se otvori problematika sagledavanja parazitskih zračenja, kako induktivnih, tako i konduktivnih, koja vrše uređaji za prenos podataka i njihovi sklopovi.*

Problem elektromagnetnog zračenja, kao nekorisnog, ali i neizbežnog dela rada svih elektronskih i električnih uređaja, pa samim tim i onih koji služe za kriptoobradu informacija, moguće je sagledati i pokušati smanjenje štetnih emisija, samo uz dobro poznavanje principa nastajanja istih.

Ključne reči: *Zračenje, Prisluškivanje, Sigurnost informacija*

1. UVOD

Interesovanje o elektromagnetskom zračenju (EMR) i elektromagnetnom prisluškivanju je fenomen koji datira unazad više od dvadesetak godina dok je u SAD ovom problemu počelo da se intenzivnije razmišlja još pre više od četrdeset godina. Skoro sve armije sveta i obaveštajne agencije su oduvek znale da elektromagnetni uređaji, bez odgovarajuće zaštite, generišu visoki nivo signala radio frekvencije (RF) koji se mogu snimiti i posebnim često jednostavnim metodama pretvore u jasne i otvorene informacije. Zato što nedostaju stručna saznanja koja se odnose na temu i opasnost u vezi Kompromitujućeg Elektro Magnetnog Zračenja (KEMZ), ovoj problematici nedovoljno je posvećivana pažnja, a posebno u oblasti računarske tehnologije.

Pojava masovnog korišćenja opreme informacione tehnologije sa informacijama od velike osetljivosti i značaja ističe u prvi plan problem za štite državnih, vojnih, i drugih tajni. Problem neovlašćenog pristupa informacijama putem KEMZ je prisutan u vojnim, diplomatskim i obaveštajnim krugovima više od 40 godina. U zapadnoj literaturi se ova problematika naj češće podvodi pod akronim američke vlade TEMPEST (*Transient Electro Magnetic Pulse Emanation Standard*), mada se javljaju i tvrdnje da je to samo kodni naziv bez nekog posebnog značenja. U svakom slučaju, radi se o strogo poverljivim standardima koji definišu dozvoljene granice i metode merenja TEMPEST-a odnosno KEMZ-a.

Pojam *kompromitujućeg zračenja* kod nas prevashodno se vezuje za uređaje na kojima se vrši kriptozaštita informacija.

Kod uređaja za kriptoobradu informacija, koji se primenjuju u oblasti kriptozaštite, zaštićena informacija je prisutna na ulazu u uređaj (šifrovanje), ili na njegovom izlazu (dešifrovanje).

U navedenim slučajevima uređaj vrši ili transformaciju tajne informacije u šifrat, koji se prenosi telekomunikacionim kanalom, ili njoj inverznu transformaciju šifrata u otvorenu informaciju. U tim postupcima transformisanja informacije iz jednog u drugi oblik, odnosno u svim slučajevima kada je tajna informacija prisutna u uređaju u formi elektromagnetnog signala, dolazi do emitovanja parazitske elektromagnetske energije korelisane sa kriptološki štićenom informacijom.

U širem kontekstu posmatranja ove problematike, KEMZ se odnosi i na uređaje na kojima se ne vrši kriptozaštita informacija kao što je između ostalog i slučaj sa informatičkom opremom komercijalnog tipa.

Po svojoj prirodi KEMZ je pojava ista kao i ostale elektromagnetne smetnje. Razlika je jedino u tome što se radi o signalima koji nose informaciju koja ne sme biti dostupna nepozvanim licima, odnosno, ne sme biti prisluškivana. Nivo signala koji može da se prisluškuje je znatno niži od nivoa signala koji potencijalno mogu ometati rad drugih uređaja, pa je problem sprečavanja kompromitujućeg elektromagnetnog zračenja teže rešiti od problema elektromagnetske kompatibilnosti. Međutim, mehanizmi nastajanja obe vrste signala su u potpunosti jednaki i ustaljena je praksa da se ove pojave zovu smetnjama.

2. ZAHTEVI ELEKTROMAGNETNE ZAŠTITE

Sve osetljiviji elektronski uređaji i sistemi moraju pouzdano da rade u uslovima delovanja mnogobrojnih prirodnih i veštačkih izvora elektromagnetnih smetnji i istovremeno ne smeju biti uzrok nenamernog ometanja ostalih sopstvenih elektronskih sredstava i sistema i izvor KEMZ-a.

Efekti i posledice delovanja mnogobrojnih prirodnih i veštačkih izvora smetnji direktno su povezani sa različitim ulogama i funkcijama elektronskih uređaja u raznim elektronskim i borbenim sistemima, a cena primene adekvatnih tehničkih rešenja srazmerna je stepenu ranjivosti istih, kao i značaju datog sredstva ili tehničkog proizvoda , odnosno uopšte tehničkih proizvoda bez obzira na kom se nivou upotrebljavaju. Rešavanje ove problematike u celini može se označiti opštim terminom "elektromagnetska zaštita" a prema specifičnostima svakog od navedenih problema, nalaženje odgovarajućih tehničkih rešenja obavlja se u okviru sledećih oblasti:

1. Elektromagnetska kompatibilnost,
2. Zaštita od jakih EM polja,
3. Zaštita od elektromagnetskog impulsa nuklearne eksplozije i elektromagnetske bombe,
4. Kompromitujuća elektromagnetska zračenja,
5. Zaštita od atmosferskih pražnjenja (udara groma) i
6. Zaštita od elektrostatičkih pražnjenja.

Svaka od ovih oblasti ističe različite tipove izvora i prijemnika smetnji i na nju se primenjuje odgovarajući standard. Kada se radi o sredstvima i složenim tehničkim sistemima, celishodno je sve ove zahteve, koje karakterišu isti zakoni generisanja, prostiranja i delovanja, integralno posmatrati i rešavati. Pri tome ne treba privilegovati jedan određen aspekt bez razmatranja ostalih, što može rezultirati nepotrebnim predimenzionisanjem, dati lažan utisak pouzdane zaštite i povećati cenu sredstva.

Nenamerno ometanje rada sopstvenih elektronskih uređaja nije jedini problem prouzrokovan parazitnim emisijama. Kada se radi o uređajima za kriptozaštitu, prenos, obradu, prikaz ili memorisanje poverljivih informacija, pokazalo se da njihove parazitne emisije u nekim frekvencijskim opsezima specifičnim za svaki uređaj, sadrže modulaciju koja se može detektovati sa znatne udaljenosti i dekodovati u čitljivu informaciju.

Elektronsko prisluškivanje putem ovakvih kompromitujućih elektromagnetskih zračenja, kao pasivna infiltracija koju je teško otkriti, predstavlja jedan od značajnih načina ugrožavanja bezbednosti, posebno za kompaktne i fizički izolovane računarske i informacione sisteme.

Od svih navedenih zahteva elektromagnetne zaštite, dva su bitna za tematiku koju tretira ovaj rad, a to su : elektromagnetska kompatibilnost i kompromitujuće elektromagnetsko zračenje.

3. ELEKTROMAGNETSKA KOMPATIBILNOST

Problem nenamernog ometanja se pojavio skoro istovremeno sa početkom primene radio-uređaja.

Izvori smetnji su bili uglavnom elektromehanički uređaji, a receptori radio-prijemnici, pa je pojava označena terminom "radio-smetnje". Jedan od prvih zabeleženih slučajeva ovakvog ometanja je dokumentovan od strane Federalne vazduhoplovne agencije SAD 1927. godine. Uočeno je da visinomer aviona daje pogrešne podatke, a uzrok su bile smetnje generisane u sistemu za paljenje motora.

Već 1934. godine, na inicijativu međunarodne elektrotehničke komisije (IEC) i mnogih drugih međunarodnih organizacija osnovan je specijalni međunarodni komitet za radio-smetnje ``CISPR`` sa primarnom funkcijom zaštite telekomunikacionih službi i radiodifuznog prijema na frekvencijama iznad 9 kHz i sprečavanja zagađenja spektra kao ograničenog prirodnog resursa.

Nakon 2. svetskog rata stalno je rastao broj i vrste službi koje koriste ili traže prostor u radio-frekvencijskom spektru. Na primer, broj mobilnih radio-uređaja se približno udvostručavao svakih 4 do 5 godina, a još brže se povećavao broj radara uz opštu tendenciju povećavanja osetljivosti prijemnika i snage predajnika, što je opet ekvivalentno povećanju broja uređaja sa aspekta nivoa smetnji na mestu prijema. Sa razvojem elektronike i sa pojavom sve većeg broja korisnika radio-frekvencijskog spektra i uređaja namenjenih za emitovanje i prijem talasa (telekomunikacioni, radio-lokacioni, radio-navigacioni sistemi itd), nastao je problem njihovog međusobnog nenamernog ometanja.

Ubrzo je termin "radio-frekvencijske smetnje" postao neadekvatan i počinje se govoriti o "elektromagnetskim smetnjama" zato što one prekrivaju i delove spektra koji se ne koriste u radio-komunikacijama, a sem radio-uređaja mogu ometati i druge osetljive elektronske uređaje.

U takvim uslovima se ukupni nivo smetnji obično toliko poveća da tehnička rešenja usmerena ka usavršavanju metoda prijema u prisustvu smetnji ne mogu da obezbede

potreban kvalitet bez ograničavanja, tj. normiranja dozvoljenog nivoa smetnji odgovarajućim standardima.

Prvi vojni standard je publikovan 1945. godine u SAD, a šezdesetih godina CISPR izdaje preporuke na osnovu kojih su izrađeni mnogobrojni civilni nacionalni standardi za dozvoljeni nivo radio-frekvencijskih smetnji komercijalnih električnih i elektronskih aparata.

Dalji razvoj elektrotehnike i elektronike doveo je do velike koncentracije raznih električnih, elektromehaničkih, radio, radarskih i drugih elektronskih uređaja na malom prostoru, naročito u vojnim sredstvima i sistemima (avioni, brodovi, tenkovi). Namena većine njih nije zračenje energije, ali zbog objektivno postojećih tehničkih nesavršenosti, sva ona u toku rada stvaraju parazitno polje u svojoj okolini (radijacione smetnje), i unose kondukcione smetnje u spojne i energetske kablove. Većina tih smetnji ima impulsni, tj. širokopojasni karakter, tako da može da blokira veliki deo spektra za prijem radio-signala, ili ometa rad drugih osetljivih elektronskih uređaja.

Primenom osetljivih poluprovodničkih elektronskih sklopova za kontrolu i upravljanje, neki dojučerašnji isključivi izvori smetnji postali su potencijalne žrtve smetnji. U stvari, neki od njih su izvori smetnji, drugi su potencijalni receptori, a treći i jedno i drugo. Nije ni tehnički ni ekonomski opravdano potpuno blokirati sve izvore smetnji, a osetljivi uređaji moraju raditi u prisustvu brojnih i snažnih radio i radarskih predajnika, bilo da su oni elementi datog sistema, bilo da pripadaju drugim sopstvenim sredstvima i sistemima koji se mogu naći u blizini. Vremenom se ovaj problem zaoštrio u meri koja je dovela do formiranja novog naučnog pravca u elektrotehnici – elektromagnetske kompatibilnosti (EMC), koja treba da omogući neophodno prestrojavanje tradicionalnih metoda projektovanja, proizvodnje i eksploatacije uređaja i sistema, objedinjujući ostale discipline elektrotehnike na bazi sistemskog pristupa rešavanju.

EMC je po svojoj definiciji "sposobnost nekog uređaja ili sistema da zadovoljavajuće funkcioniše u svojoj elektromagnetskoj okolini i da pri tome sam ne stvara nedopustive elektromagnetske smetnje bilo čemu što se nalazi u toj okolini". Drugim rečima, da bi se uspostavila EMC kada se neki uređaj ili sistem postavi u elektromagnetsku okolinu u kojoj treba da radi, ne sme da emituje prekomerne smetnje, ali istovremeno mora imati i odgovarajuću imunost na smetnje te okoline, što odavno predstavlja zahtev u EMC standardima.

Svedoci smo masovne primene računara – u velikim informacionim sistemima. Oni se uvezuju u mreže, u industriji upravljaju proizvodnim procesima, a postali su nezaobilazni deo kućnog inventara. Svake godine se u automobile ugrađuje sve više elektronskih sklopova radi veće ekonomičnosti, bezbednosti i komfora.

Njihova funkcija i uloga postaje sve složenija i važnija. Mikroprocesori nalaze široku primenu i ovde i u mnogim drugim oblastima gde je potrebna jeftina i nepogrešiva kontrola i upravljanje. Može se slobodno reći da današnje društvo zavisi od elektronike i njenih poluprovodničkih elemenata verovatno i više nego što je ljudsko društvo ikada zavisilo od bilo kakvog izuma ili proizvoda. Ali i tu su se javili ozbiljni problemi - u robotici, pri upotrebi mobilnih telefona i ostalih elektronskih uređaja

Da bi se razrešio ili bar ublažio ovaj problem, brojni komiteti i komisije IEC-a za proizvode, korisnici i proizvođači električne i elektronske opreme su morali da utvrde nivoe imunosti koje njihova oprema treba da izdrži i da razviju odgovarajuće metode ispitivanja imunosti.

Generalno, problem EMC se može posmatrati na više nivoa različitih kako po obimu tako i po složenosti, načinu i putevima delovanja smetnji, tehničkim rešenjima zaštite itd., od štampane pločice, modula, pojedinačnog uređaja i sistema do njihovog skupa na određenoj platformi ili prostoru.

Na nižim nivoima se međusobne neželjene interakcije odvijaju putem polja u bliskoj ili dalekoj zoni, kao i kondukcionim putem preko zajedničkog izvora napajanja i petlji zajedničkog uzemljenja. Na najvišem nivou posmatranja problema EMC do nenamernog ometanja dolazi isključivo preko antena, najčešće u dalekoj zoni. Uz trend stalnog povećavanja broja i snage raznih predajnika i praktično zauzet celokupni spektar kao ograničeni prirodni resurs, problem EMC svakim danom dobija sve veći značaj.

4. KOMPROMITUJUĆA ELEKTROMAGNETNA ZRAČENJA - KEMZ

Trend masovnog korišćenja opreme informacione tehnologije sa informacijama od velike osetljivosti i značaja ističe u prvi plan problem zaštite državnih, vojnih, naučnih, privrednih, poslovnih i finansijskih tajni.

Zavisno od regiona i države, problematika kompromitujućeg elektromagnetnog zračenja ima svoje ustaljene nazive kao:

- U Srbiji naziv je KEMZ,
- Americi primenjuje se termin TEMPEST, itd.

U civilnom sektoru je dugi niz godina preovladavalo mišljenje da je vrlo teško rekonstruisati podatke skrivene u parazitnim emisijama i stoga se verovalo da prisluškivanje na osnovu KEMZ mogu da obavljaju samo profesionalci koji raspolažu vrlo sofisticiranim uređajima za detekciju i dekodovanje. Kao rezultat, digitalna oprema za obradu informacija koja zahteva srednji ili niski nivo zaštite, kao što su privatne i poslovne informacije, nije štićena od prisluškivanja ove vrste. Međutim, istraživanja mogućnosti prijema i dekodovanja KEMZ koja potiču od video jedinice računara jasno su pokazala da se ovaj tip krađe informacija lako može obaviti sa priličnog rastojanja čak i sa minorno modifikovanim običnim TV prijemnikom, antenom i dodatnim jednostavnim uređajem za sinhronizaciju.

Vojnim organizacijama je bilo poznato još iz ranih 60-tih godina da računari generišu elektromagnetsko zračenje koje ne samo da pravi smetnje radio-prijemu, nego takođe odaje informacije o podacima koji se obrađuju.

Poznato kao kompromitujuće oticanje ili Tempest zračenje, kodna reč za klasifikovani istraživački program vlade SAD, elektromagnetsko emitovanje podataka bilo je zna čajna briga u osetljivim računarskim aplikacijama.

U praksi je poznat slučaj kada su pripadnici obaveštajne službe V.Britanije primetili da šifrovani saobraćaj nosi slab sekundarni signal, i konstruisali su opremu koja ga rekonstruiše. Ispostavilo se da je to otvorena informacija.

Eksperimenti sa prisluškivanjem KEMZ koja potiču od kabla RS-232 takođe su dokazali da je u nekim slučajevima moguće detektovati i dekodovati signale koji se njima prenose čak i običnim tranzistorskim prijemnikom i zabeležiti standardnim sredstvima snimanja. Signali koji se prenose sa RS-232 mogu sadržati vrlo osetljive informacije kao što su lozinke, kodovi korisnika i finansijskih transakcija i u tom smislu prisluškivanje ima značajno različite konsekvence u pogledu bezbednosti informacija.

Pojam Kompromitujućeg zračenja kod nas prevashodno je vezivan za uređaje na kojima se vrši kriptozaštita informacija. Kod uređaja za kriptoobradu tajnih informacija, koji se primenjuju u oblasti kriptozaštite, štićena informacija je prisutna na ulazu u uređaj (šifrovanje), ili na njegovom izlazu (dešifrovanje). U navedenim slučajevima uređaj vrši ili transformaciju tajne informacije u šifrat, koji se prenosi telekomunikacionim kanalom, ili inverznu transformaciju šifrata u otvorenu informaciju. U tim postupcima transformisanja informacije iz jednog u drugi oblik, odnosno u svim slučajevima kada je tajna informacija prisutna u uređaju u formi elektromagnetnog signala, dolazi do emitovanja parazitske elektromagnetske energije korelisane sa kriptološki štićenom informacijom.

U širem kontekstu posmatranja ove problematike, kompromitujuće elektromagnetno zračenje odnosi se i na uređaje na kojima se ne vrši kriptozaštita informacija kao što je između ostalog i slučaj sa informatičkom opremom komercijalnog tipa.

Po svojoj prirodi KEMZ je pojava ista kao elektromagnetne smetnje. Razlika je jedino u tome što se radi o signalima koji nose informaciju koja ne sme biti dostupna okolini, tj. ne sme biti prisluškivana. Nivo signala koji može da se prisluškuje je znatno niži od nivoa signala koji potencijalno mogu ometati rad drugih uređaja, pa je problem sprečavanja kompromitujućeg elektromagnetskog zračenja teže rešiti od problema elektromagnetske kompatibilnosti. Međutim, mehanizmi nastajanja obe vrste signala su u potpunosti jednaki i ustaljena je praksa da se ove pojave zovu smetnjama.

5. ZAKLJUČAK

Kompromitujuća elektromagnetna zračenja (KEMZ) predstavljaju problem kada je u pitanju oticanje informacija (radio-praćenje, elektro mreža napajanja i mreža uzemljenja).

Savremena digitalna tehnika, pa samim tim i PC računari, nije imuna na neželjena EM zračenja.

Rad na zaštiti od KEMZ-a zahteva angažovanje visoko stručnih lica i adekvatnu mernu opremu.

Ovo je samo jedan pristup sagledavanju izvora smetnji putem elektromagnetnog zračenja. Ostaje dosta prostora za dalju nadogradnju teoretskih saznanja, kao i praktičnih istraživanja na ovom polju, uz napomenu da masovna primena računarske komunikacije nužno iziskuje posebnu pažnju, kako zračenja elektronskih elemenata i sklopova, tako i terminalnih uređaja.

LITERATURA:

1. А.А.Хорев, *Способы и стедства защиты информации, учебное пособие*, МО РФ, Москва, 1998 г.

2. Е. С. Бландова, *Помехаподавляющие изделия. Рекомендации по выбору и применению*, Специалъая техника, 2001. г.

3. M.Kuhn., R.Anderson, *Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations,* 2004.

TEMPEST AND INFORMATION SECURITY

Abstract: *The aim of this paper is to open the consideration of problems of parasitic radiation, as inductive, and konduktivnih which perform data transmission devices and their components.*

The problem of electromagnetic radiation, such obsolete but inevitable part of all electronic and electrical devices, and therefore and those who serve encryption information, it is possible to observe and try to reduce harmful emissions, only with a good knowledge of the principles of the same.

Key words: *Radiation, surveillance, information security*