

ODREĐIVANJE KEMZ OBELEŽJA NA PC OPREMI U TEMPEST IZVEDBI ZONE 0 I ZONE 1

mr Branislav Lučić, dipl.ing, Jugoimport SDPR, Beograd, b_tempest@EUnet.yu

Apstarkt: *U ovom radu opisuju se rezultati istraživanja o mogućem prisluškivanju sa video-displej jedinica (VDU-a, Z1 i Z0), preko prijema i interferencije elektromagnetskih talasa, koje generiše ovaj tip uređaja.*

Ključne reči: *Elektromagnetsko zračenje, prisluškivanje, sigurnost podataka, privatnost, elektromagnetska kompatibilnost.*

DETERMINATION COMPROMISING EMANATION TO PC EQUIPMENT TEMPEST PRODUCTS FOR ZONE 0 AND ZONE 1

Absract: *This paper describes the results of research into the possibility of eavesdropping on video display units (VDU, Z1 end Z0), by piching up and decoding the electromagnetic interference produced by this type of equipment*

Key words: *Electromagnetic radiation, eavesdropping, data security, privacy, electromagnetic compatibility.*

1. UVOD

Sadašnji rašireni interes o elektromagnetskom zračenju (EMR) i elektromagnetnom prisluškivanju je fenomen koji nije od skora. Za više od dvadeset godina (u SAD više od četrdeset godina), međunarodna vojska i obaveštajne agencije su znale da svi elektromagnetni uređaji, bez odgovarajuće zaštite, generišu visoki nivo signala radio frekvencije (RF) koji se mogu "uhvatiti" i rekonstruisati u čitljive informacije.

Zbog opšteg nedostatka saznanja koje se odnosi na teme i opasnost u vezi TEMPEST-a tj. **Kompromitujućeg ElektroMagnetskog Zračenja (KEMZ)**, ovoj problematici nedovoljno je posvećivana pažnja, a posebno u oblasti informatičke tehnologije.

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. Problematika neovlašćenog pristupa informacijama putem KEMZ je prisutna u vojnim, diplomatskim i obaveštajnim krugovima više od 30 godina. U zapadnoj literaturi se ova problematika najčešće podvodi pod akronim američke vlade TEMPEST (**T**ransient **E**lectro**M**agnetic **P**ulse **E**manation **S**Tandard) [1], [2], mada ima tvrdnji da je to samo kodni naziv bez nekog posebnog značenja [3]. 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 je vezivan za uređaje na kojima se vrši kriptozastita informacija.

Kod uređaja za kriptu obradu tajnih informacija, koji se primenjuju u oblasti kriptozastite, 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 kanalom veze, ili inverznu transformaciju šifrata u prvobitnu informaciju. U tim postupcima transformisanja informacije iz jednog u drugi oblik, odnosno u svim slučajevima kada je tajna informacija prisutna u uređaju u formi elektromagnetskog signala, dolazi do emitovanja parazitske elektromagnetske energije korelisane sa kriptološki štićenom informacijom.

U širem kontestu posmatranja ove problematike, **Kompromitujuće EM Zračenje** odnosi se i na uređaje na kojima se ne vrši kriptozastita informacija kao što je između ostalog i slučaj sa informatičkom opremom komercijalnog tipa (komercijalna PC tehnologija).

Po svojoj prirodi KEMZ je pojava ista kao elektromagnetske 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.

Samo u slučajevima potrebe naglašava se razlika između signala koji nose informaciju koju treba zaštititi i ostalih smetnji.

Cilj ovog rada su pristupi da se ispituju karakteristike KEMZ-a sa relevantnim diskriminatornim obeležjima za radijacioni i kondukcioni KEMZ kod PC opreme, sa posebnim osvrtom rezultata na PC računar sa TFT monitorom.

2. PC OPREMA U IZVEDBI TEMPEST ZONE 1 I ZONE 0

Predmet ispitivanja – Merenje KEMZA je PC oprema u **TEMPEST** izvedbi **ZONE 0** i **ZONE 1**, uzorci gotovog proizvoda: PC računari (Kućišta Desktop (PC-D Z0, Z1); Monitori 15" TFT Z0, Z1; Tastature Z0, Z1 i Miš Z0, Z1), Štampač Z0 i Skeneri u izvedbi Z1.

Cilj ispitivanja i merenja je da se ispitaju karakteristike KEMZ-a sa relevantnim diskriminatornim obeležjima za radijacioni i kondukcionni KEMZ.

3. PUTEVI OTICANJA INFORMACIJA I SCENARIO NAPADA

Napravljena je Analiza mogućih puteva oticanja informacija (predikcija) i predviđen je Scenario napada za celine (PC Tempest oprema u izvedbi *ZONE 0* i *ZONE 1*) sa ciljem provere ispunjenja zahteva zaštite od KEMZ.

Na osnovu Analize i Scenarija napada određena su mesta merenja radijacionog i kondukcionog KEMZ, u cilju ponovljivosti detektovanih diskriminatornih obeležja KEMZ-a.

3.1 Putevi oticanja informacija

- 3.1.1. Izvori elektromagnetskih smetnji u električnom uređaju
- 3.1.2. Provodnik za uzemljenje kao izvor kondukcionih smetnji
- 3.1.3. Prodiranje polja kroz metalni oklop uređaja
 - 3.1.3.1. Efikasnost oklopa za električno polje
 - 3.1.3.2. Efikasnost oklopa za magnetsko polje
 - 3.1.3.3. Prodiranje ravanskog talasa kroz oklop
- 3.1.4. Prodiranje polja kroz otvore i pukotine na kućištu
- 3.1.5. Prodiranje polja preko izbočina na oklopu
- 3.1.6. Prodiranje polja preko vodova
- 3.1.7. Interakcije putem sprezanja sa sistemom za uzemljenje u cilju izdvajanja signala informacije
 - 3.1.7.1. Sprege posredstvom elektromagnetskog polja
 - 3.1.7.2. Kondukcione sprege sa provodnicima
 - 3.1.7.3. Sprege sa provodnicima posredstvom polja
 - 3.1.7.4. Kondukciona sprege sa zemljom

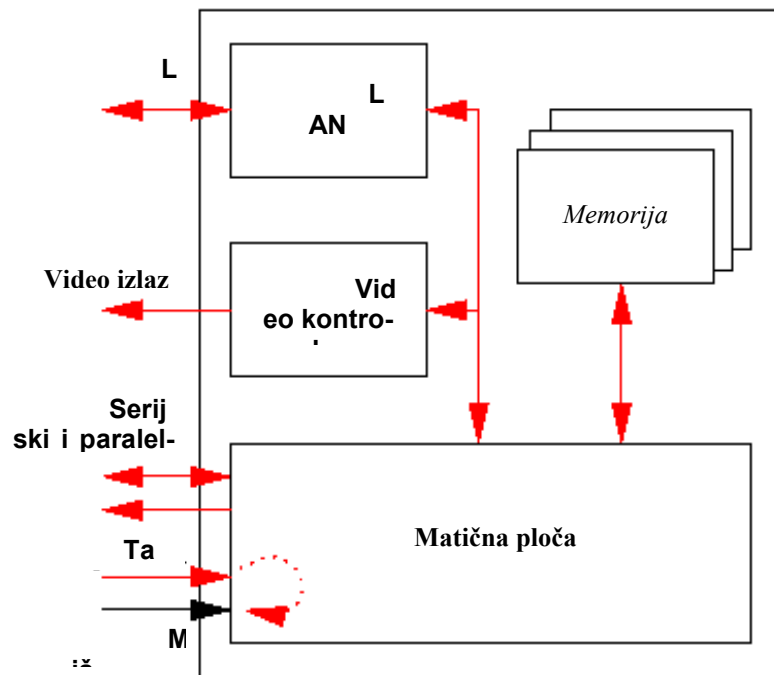
3.2 Scenario napada

Scenario napada se odnosi na pojedinačne celine koje su predmet ispitivanja, kao pojedinačni uređaji i kao sistem i to:

- a) Računari (Z0, Z1), monitori (Z0, Z1), štampač (Z0) i skener (Z1),

3.2.1 Računar

Na slici 1 dat je prikaz uprošćenih tokova signala kod računara koji utiču na ocenu ispunjenja zahteva od KEMZ.



utiču na ocenu ispunjenja zahteva od KEMZ

Ključna obeležja obuhvataju:

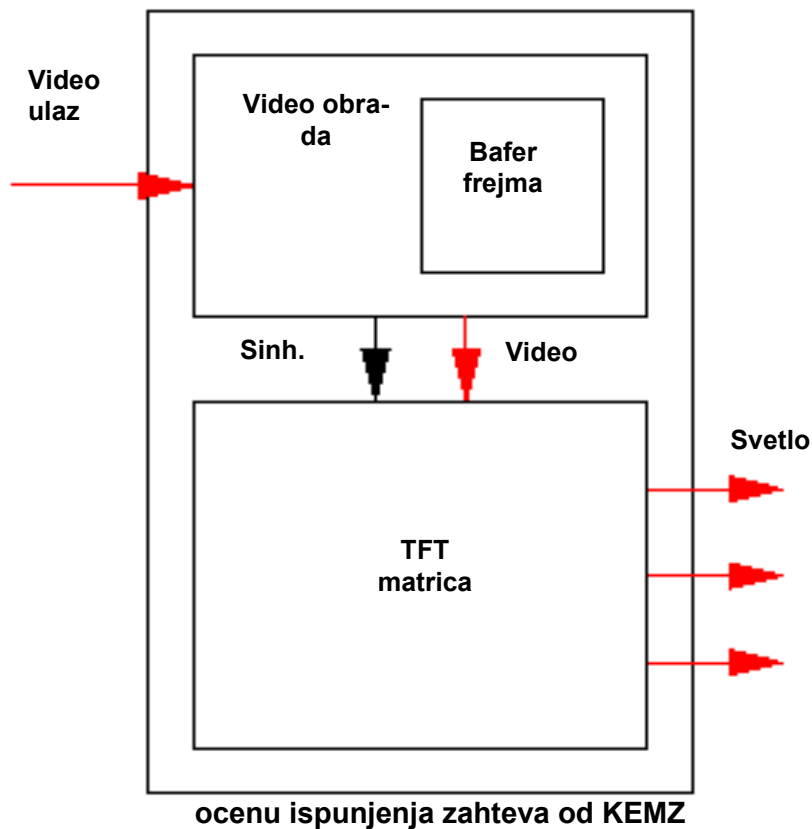
- **Serijski i paralelni I/O**
- LAN portovi
- Čitanje / upis – glavne serijske informacije
- **Port monitora**
- **Podaci sa tastature**
- **Miš: kao antena za signale tastature**

3.2.2 Monitor

Na slici 2. dat je prikaz signala kod monitora koji utiču na ocenu ispunjenja zahteva od KEMZ.

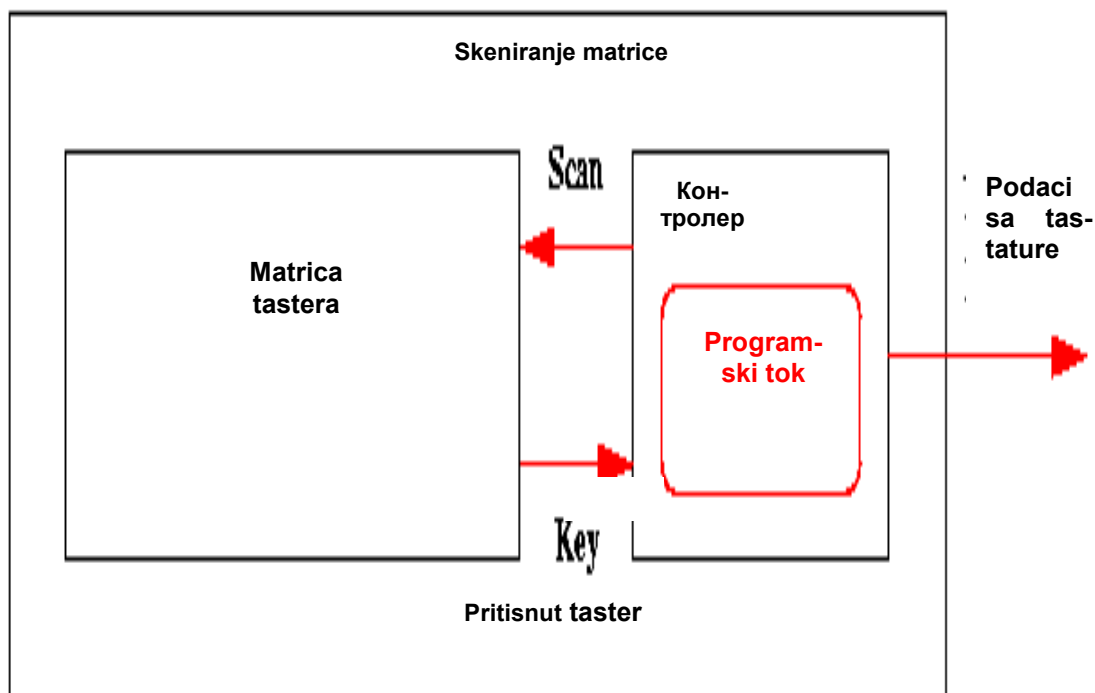
Ključna obeležja obuhvataju:

- **Dolazeći video podaci**
- TFT: Re-odabrani video podaci (Ploča)
- **CRT: Prenešeno svetlo**
- Poboljšanje SNR zbog ponavljanja slike:
- $SNR = O(\sqrt{\text{br. slika}})$
- Frekvencija frejma 80 Hz, 60 sekundi daje 4800 slika
- 4800 slika daje SNR poboljšan za faktor 69



3.2.3 Tastatura

Na slici 3. dat je prikaz signala tastature koji utiču na ocenu ispunjenja zahteva



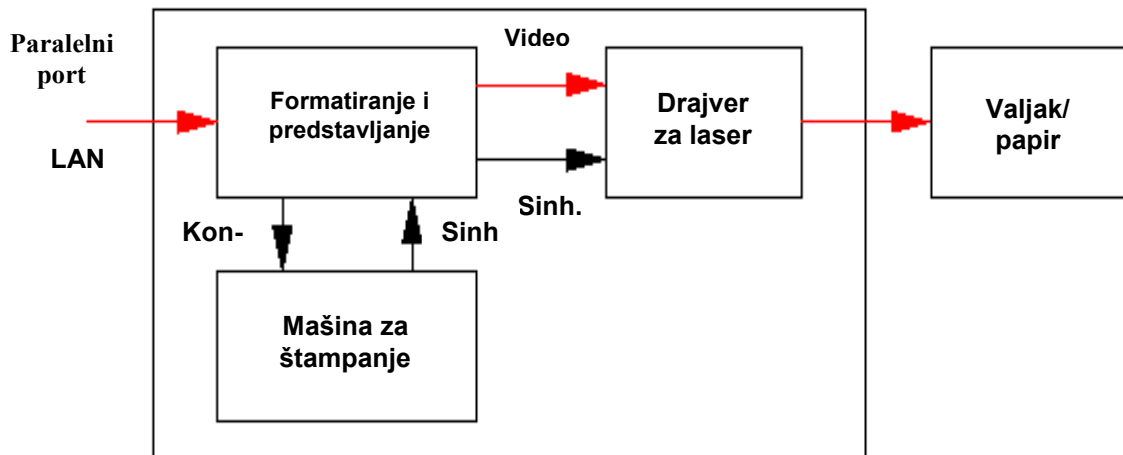
Slika 3. Prikaz signala tastature koji utiču na ocenu ispunjenja zahteva od KEMZ

Ključna obeležja obuhvataju:

- **Serijski podaci tastature**
- Matrica skeniranja tastature
- Širokopojasni signal sa kontrolera (iz programskog toka)
-

3.2.4 Štampači

Na slici 4. dat je prikaz signala štampača koji utiču na ocenu ispunjenja zahteva od



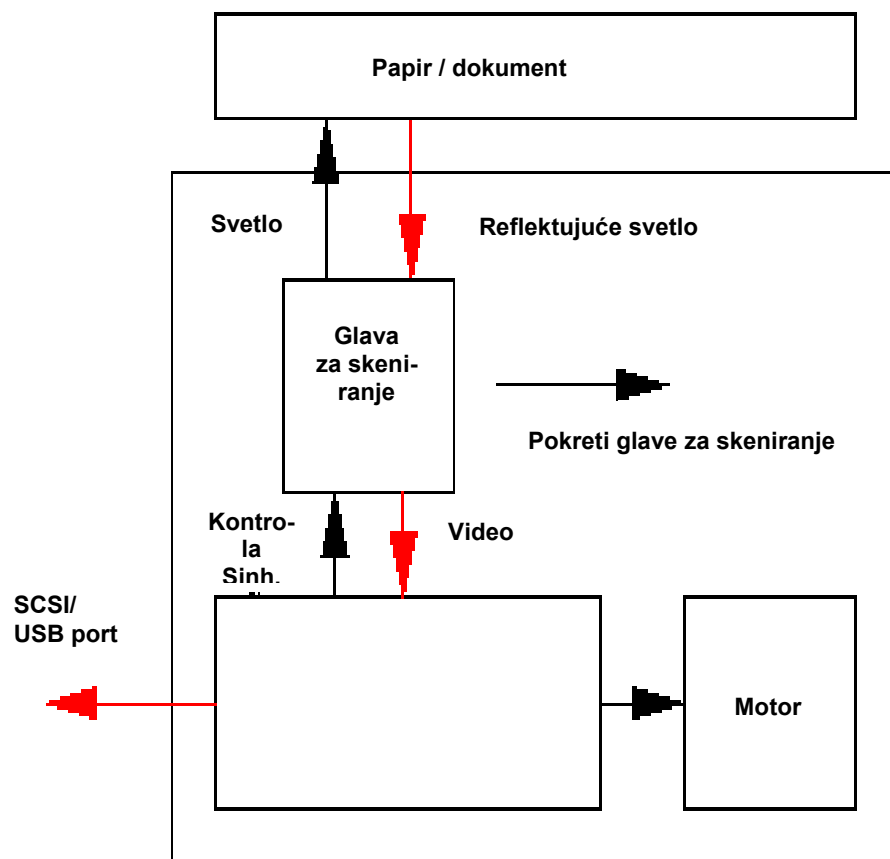
Slika 4. Prikaz signala štampača koji utiču na ocenu ispunjenja zahteva od KEMZ.

Ključna obeležja obuhvataju:

- **Paralelni izlaz za podatke**
- Serijski podaci lasera, ili podaci glave za štampanje
- **Uzemljenje**

3.2.5 Skeneri

Na slici 5. dat je prikaz signala skenera koji utiču na ocenu ispunjenja zahteva od KEMZ.



Slika 5. Prikaz signala skenera koji utiču na ocenu ispunjenja zahteva od KEMZ.

Ključna obeležja obuhvataju:

- Slika podataka sa senzora
- Podaci sa porta ka računaru
- Uzemljenje

4. MERENJA

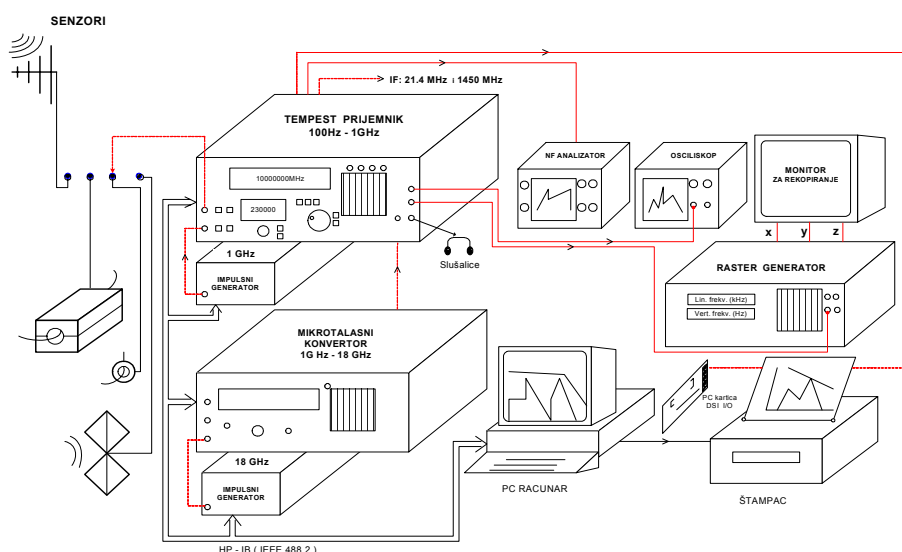
Na slici 6 prikazana je postavka šeme za merenje KEMZ-a i rekonstrukcije slike sa PC računara gde se za prikaz merenja KEMZ-a i rekopiranja VDU-a koristi profesionalna oprema.

Za kvalitetan prijem (detekciju) je neophodan prijemnik sa mogućnošću izbora širokih propusnih opsega. Odabiranje najpogodnije širine propusnog opsega je uvek kompromis između integriteta detektovanog signala i nivoa šuma.

Za rekonstrukciju su se pored **prijemnika** koristili **monitor PC** iz mernog sistema i **raster generator** (horizontalni i vertikalni sinhrogenerator) za simulaciju frekvencije horizontalne sinhronizacije i frekvenciju ponavljanja slike. Raster generator ima takve karakteristike da u sprezi sa širokopojasnim prijemnikom i monitorom može da da vizuelni prikaz skoro svih periodičnih signala (monitori računara, terminali, TV, ...).

U postupku rekonstrukcija slike PC na osnovu KEMZ u realnim uslovima, moguća su dva pristupa:

- U drugom slučaju, kada nisu poznate karakteristike ciljnog računara sa stanovišta KEMZ, postupak se realizuje u par iteracija.



Za potrebe predviđanja daljine detekcije **Kompromitujućeg EM Zračenja**, razvijeni su softverski alati, kada su predhodno merenja KEMZ na predmetnom PC-u obav-

ljena u Faradejevom kavezu na udaljenosti 1 m, uz procenu rastojanja na kojem nivo Kompromitujućeg EM Zračenja opadne na još uvek detektabilni nivo od **1 μ V/m/MHz**.

5.1 TEMPEST PC oprema **ZONE 1 (Z1)** i **ZONE 0 (Z0)**

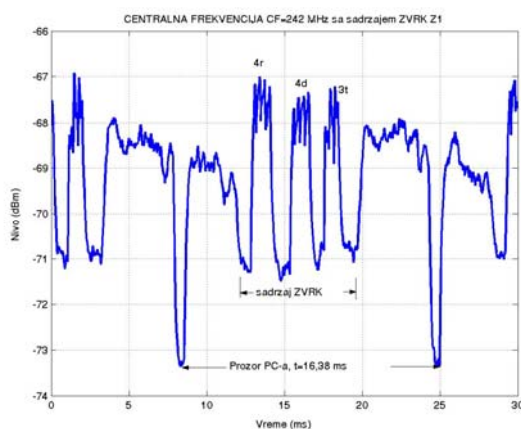
Ispitivan je zasebno: PC računar (Z0, Z1) i komplet: PC računar (Z1) + Skener (Z1) + Štampač (Z0).

Merenja su obavljena u frekventijskom opsegu od 100 Hz do 1500 MHz. Merne antene nalazile su se na udaljenosti 1 m od predmetnog VDU-a i posebnih celina PC opreme.

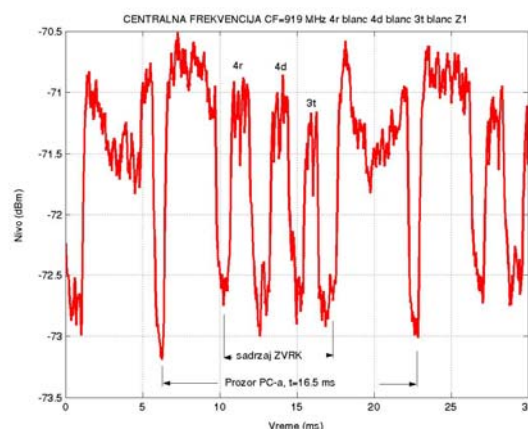
Na slikama 7 i 8 prikazan je dominantan sadržaj (karakterističan) ciljnog VDU-a (TFT monitor) u vremenskom domenu (pretraživanja i određivanje diskriminacionih obeležja su vršena u frekventijskom domenu, a prikaz rezultata je dat u vremenskom domenu).

Na slici 7 je prikazan signal radijacionih parazitnih zračenja u frekventijskom opsegu od 50 MHz do 300 MHz sa slovnom test signalom na ekranu, rutina ZVRK (4 reda slova **r**, 4 prazna reda, 4 reda slova **d**, 4 prazna reda, 3 reda slova **t**, i 3 prazna reda).

Na slici 8 je prikazan signal u vremenskoj domeni radijacionih parazitnih zračenja u frekventijskom opsegu od 50 MHz do 1000 MHz sa slovnom test signalom na ekranu, rutina ZVRK (4 reda slova **r**, 4 prazna reda, 4 reda slova **d**, 4 prazna reda, 3 reda slova **t**, i 3 prazna reda).



Slika 7. Prikaz signala radijacionog parazitnog zračenja sa sadržajem rutine ZVRK



Slika 8. Prikaz signala radijacionog parazitnog zračenja sa sadržajem rutine ZVRK

NALAZ:

1. U frekventijskom opsegu od 50 MHz do 1200 MHz registrovana su diskriminatorska obeležja KEMZ-a.
2. Registrovana diskriminatorska obeležja KEMZ-a za predmetnu Tempest opremu u izvedbi ZONE 1 mogu se detektovati do udaljenosti 100 m, a za Tempest opremu u izvedbi ZONE 0 do udaljenosti 5m.

6 ZAKLJUČAK

Za predmetnu Tempest opremu u izvedbi *ZONE 1* i *ZONE 0* u frekvencijskom opsegu od 50 MHz do 1200 MHz registrovana su diskriminatorna obeležja KEMZ-a. Registrovana diskriminatorna obeležja KEMZ-a u izvedbi *ZONE 1* mogu se detektovati do udaljenosti 100 m, a u izvedbi *ZONE 0* do 5m udaljenosti.

Sobzirom da se predmetna oprema predviđa za korišćenje u prostoru koji nije EM ekranizovan, treba voditi računa o sledećem:

- Efekat ekranizacije zgrada na zračenje je vrlo promenljiva veličina koja zavisi od materijala zgrada, debljine zidova i veličine prozora. Za pune zidove bez prozora, slabljenje zavisi od njihove debljine u odnosu na talasnu dužinu zračenja i može se očekivati povećanje slabljenja sa porastom frekvencije.
- Po pravilu se ne očekuje da zgrada pruža zaštitu znatno veću od 10 do 15 dB.

LITERATURA

1. H.J. Higland, *"The Tempest over Leaking Computers"*, ABACUS, Vol. 5, No. 2, pp. 10-18, 1988,
2. Kultsar E., *"Design Geometry for Enclosure Shielding"*, EMC Test & Design, pp. 33-34, Aug.t 1993.
3. Mauriello A.J., *"Join a Government Program to Gain Tempest Expertise"*, EMC TECHNOLOGY, pp. 25-27, 64, July-Sept. 1984
4. Lučić D. B., Rezultati merenja na različitim tipovima VDU-a, TOC Beograd, 1994-2005.
5. Lučić D. B., *"Programi za predviđanje i određivanje maksimalne udaljenosti detekcije KEMZ, kada je merenja na predmetnom PC obavljena na 1m u Faradejevom kavezu"*, TOC Beograd, maj 2000.
6. Lučić D. B., Jovanovic V. B., *"Ispitivanje kvaliteta sredstava NVO i tehničkih proizvoda, metode merenja i metrološko obezbeđenje"*, ZBORNIK RADOVA NAUČNO-STRUČNOG SKUPA, Beograd, decembar 2003.
7. Lučić D. B., Jovanović V. B. *Prvo savetovanje o zloupotrebama u informacionim tehnologijama – ZITEH*, Tara 31.05. do 03.06.2004.
8. Lučić D. B., *"Mehanizmi oticanja informacija putem kompromitujućeg elektromagnetskog zračenja i principi zaštite na personalnim računarima"*, Magistarski rad, (2004), FTN Novi Sad.
9. Lučić D. B., . Prvi NAUČNI SKUP, *ODBRAMBENE TEHNOLOGIJE U FUNKCIJI MIRA*, Beograd 6 do 7. decembar 2005. godine