

МЕРЕЊЕ ПАРАЗИТНИХ ЕМ ЗРАЧЕЊА НА РС РАЧУНАРИМА РИЗИК ОД ПРИСЛУШКИВАЊА И ЗЛОУПОТРЕБА

MEASUREMENTS OF COMPROMISING RADIATION FROM PC UNITS: AN EAVESDROPPING RISK AND MISUSE

пуковник Бранислав Лучић, дипл. инж.

Биљана Јовановић, дипл. инж.

Технички Опитни Центар КоВ, 11000 Београд, Војводе Степе 445

Резиме: Садашњи раширени интерес и запрепашћење о електромагнетном зрачењу (ЕМР) и електромагнетном прислушкивању је феномен који није од скоро. Већ више од двадесет година, међународна војска и обавештајне агенције су знале да сви електронски уређаји, без одговарајуће заштите, генеришу висок ниво сигнала радио фреквенције (РФ) који се могу "ухватити" и реконструисати у читљиве информације.

У овом раду описују се резултати истраживања о могућем прислушкивању са видео-дисплеј јединица (VDU-a), преко пријема и интерференције електромагнетских таласа, које генерише овај тип уређаја.

КЉУЧНЕ РЕЧИ: ЕЛЕКТРОМАГНЕТСКО ЗРАЧЕЊЕ, ПРИСЛУШКИВАЊЕ, СИГУРНОСТ ПОДАТАКА, ПРИВАТНОСТ, ЗЛОУПОТРЕБА, ЕЛЕКТРОМАГНЕТСКА КОМПАТИБИЛНОСТ

Abstract: The current widespread interest and dismay over electromagnetic radiation (EMR) and electromagnetic eavesdropping might suggest that these are now phenomena or at least were recently discovered. For more than twenty years, international military and intelligence agencies have known that all electronic equipment without suitable shielding generates high levels of radio frequency (RF) signals that can be intercepted and reconstituted into intelligible information.

This paper describes the results of research into the possibility of eavesdropping on video display units, by picking up and decoding the electromagnetic interference produced by this type of equipment.

KEY WORDS: ELECTROMAGNETIC RADIATION, EAVESDROPPING, DATA SECURITY, PRIVACY, MISUSE, ELECTROMAGNETIC COMPATIBILITY.

1. УВОД

Сви електронски, електрични и електромеханички уређаји при обради тајних информација због својих техничких несавршености генеришу **паразитно електромагнетско (ем) поље** у својој околини и прикључним кабловима у

спектралном опсегу, односно преносним путевима који нису предвиђени основном наменом уређаја.

Једним делом та паразитна зрачења нису везана за информативни садржај и представљају само **ем** сметње. Међутим, постоје и она на основу којих се може, извршити детекција и екстракција

обрађиване "тајне" информације. Стога се ова **паразитна ем зрачења** називају **Компромитујућа ЕМ Зрачења**.

Начин простирања је основна особина према којој се врши подела **Компромитујућег ЕМ Зрачења**. Тако се говори о кондукционом, радијационом и комбинованом **Компромитујућем ЕМ Зрачењу**.

Кондукционо означава **Компромитујуће ЕМ Зрачење** које се простира проводницима, укључујући кола са компонентама са сконцентрисаним параметрима као што су калемови, кондензатори и трансформатори.

Компромитујуће ЕМ Зрачење које се простира, путем **ем** поља укључујући и случај блиске зоне односно индукције назива се радијационо. Строго говорећи у највећем броју случајева ради се о комбинованом преносу овог типа зрачења, с обзиром да се проводник са струјом понаша као емисиона антена и обрнуто, да електромагнетско поље индукује струју у проводницима. Међутим, у пракси се најчешће, већ према томе који од начина простирања је доминантан, **Компромитујуће ЕМ Зрачење** означава као кондукционо или радијационо.

Појам **Компромитујућег ЕМ Зрачења** и заштита превасходно је везивана за уређаје на којима се врши крипто заштита информација.

Код уређаја за крипто обраду тајних информација, који се примењују у области крипто заштите, штићена информација је присутна на улазу у уређај (шифровање), или на његовом излазу (дешифровање). У наведеним случајевима уређај врши или трансформацију тајне информације у шифрат, који се преноси каналом везе, или инверзну трансформацију шифрата у првобитну информацију. У тим поступцима трансформисања информације из једног у други облик, односно у свим случајевима када је тајна информација присутна у уређају у форми електромагнетског сигнала, долази до емитовања паразитске електромагнетске

енергије корелисане са криптолошки штићеном информацијом.

У ширем контексту посматрања ове проблематике, **Компромитујуће ЕМ Зрачење** односи се и на уређаје на којима се не врши крипто заштита информација као што је између осталог и случај са информатичком опремом комерцијалног типа (комерцијална ПЦ технологија).

У САД проблематика која се односи на компромитујуће електромагнетско зрачење регулисана је TEMPEST процедурама, под ингиренцијом Владе САД.

TEMPEST је кодна реч Владе САД која означава класификован скуп стандарда за ограничавање отицања електричног или електромагнетског зрачења из електричног уређаја.

2. МОГУЋНОСТ ПРИСЛУШКИВАЊА СА ВИДЕО-ДИСПЛЕЈ ЈЕДИНИЦЕ (VDU)

Чињенично је стање да се многе државне структуре опремају са ПЦ рачунарима комерцијалне изведбе на којима нису предходно извршена **превентивна мерења** са циљем селекције и одабира ПЦ рачунара са јако малим паразитским електромагнетским зрачењем (VDU јединице типа **VLR**– врло мало зрачење).

Наша истраживања са потврђеним мерењима на елементима рачунарских система показала су да је доминантан извор **Компромитујућег ЕМ Зрачења** видео терминал (VDU), односно катодна цев и процес освежавања садржаја екрана, и то у широком фреквенцијском опсегу од HF до UHF подручја. Висок ниво **Компромитујућег ЕМ Зрачења**, на основу кога може да се реконструише садржај екрана користећи чак и неспецијализовану опрему (антену и ТВ пријемник са подешавањем синхронизације), је слабост стандардних видео дисплеј јединица без обзира на тип произвођача (Hewlett Packard, Philips, IBM, DTK, Dell, COMPAQ итд.).

Како је релативно једноставно да се реконструише информација (са адекватном мерном опремом) из поља зрачења видео дисплеј јединице (VDU), ово има директно негативне последице на безбедност тајних информација које се обрађују на предметном ПЦ.

Коментаре везано за "сигурност" употребе лаптоп и ноте боок рачунара, потребно је посматрати у светлу чињенице: "Ако су рачунари овог типа безбедни, зашто би на тржишту постојали рачунари овог типа урађени по TEMPEST стандарду".

3. УЗРОЦИ И ЕФЕКТИ

Примена прекидаких дигиталних сигнала на високим фреквенцијама, у дигиталним уређајима, доводи до зрачења **ЕМ** поља, које садржи компоненте фреквенција до UHF подручја. Такође спектрална густина снаге ових сигнала опада са повећањем фреквенције. Ово је компензовано у пољу зрачења, јер се ефекти зрачења у електричним колима унутар уређаја појачавају са порастом фреквенције. Ово значи да се ниво зрачења може сматрати константним до неколико стотина МНz.

У неким случајевима, резонанције у колима могу да доведу до вишег нивоа зрачења на неким фреквенцијама спектра зрачења (пример: коло зрачења мрежног кабла, као дела уређаја).

Ако се ограничимо на видео дисплеј јединице, веома једноставно ћемо препознати да се **ЕМ** поље зрачења дигиталних уређаја састоји од две различите компоненте:

- ускопојасне, хармоника од дигиталног такт сигнала, и
- широкопојасне, хармоника од различитих случајних дигиталних сигнала, као што је видео-сигнал.

Супротно од других широкопојасних сигнала, унутар видео дисплеја, видео сигнал се појачава од TTL нивоа, до неколико

стотина волти, пре него што се доведе на катодну цев (CRT).

Зрачење које потиче од видео сигнала, може да буде доминантна компонента широкопојасног поља, које у већини случајева генерише видео дисплеј. Сваки израчен хармоник видео сигнала показује приметну сличност са ТВ сигналом. На тај начин могуће је реконструисати слику са видео дисплеј јединице из поља зрачења мреже VDU-a.

Ако нису извршена превентивна мерења, прислушкивање видео јединица могуће је успешно вршити на дистанци од неколико стотина метара. Коришћењем чак и ТВ-пријемника и усмерених антена, са антенским појачавачима могуће је реконструисати садржај VDU-a и на дистанцама преко 1 км. Ако се користе сложенији пријемни и декодујући уређаји, дистанце могу да буду много веће.

Евидентно је да ова могућност има импликација на методе високе заштите информација. Ово је специјално релевантно, у случајевима где су превентивна мерења већ предузета, као што су енкрипција или физичка заштита.

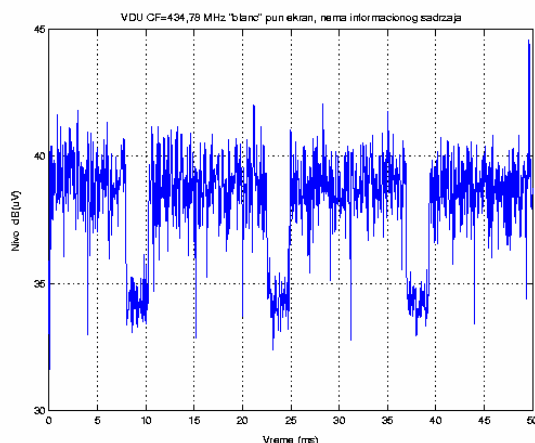
4. МЕРЕЊЕ И РЕЗУЛТАТИ

Извршена су мерења нивоа **Компромитујућег ЕМ Зрачења** испитних ПЦ (комерцијалног типа) у Фарадејевом кавезу (на 1м и 3м), као и одређивање максималних растојања на којима је могућа реконструкција слике екрана (VDU-a) испитиваних ПЦ рачунара.

У интерактивном начину рада, поред мерења нивоа радијационог зрачења вршена је истовремена идентификација фреквенцијских опсега **Компромитујућег ЕМ Зрачења**, односно дискриминација паразитних емисија које у себи садрже информацију коју треба штитити и паразитних емисија које представљају обичне сметње.

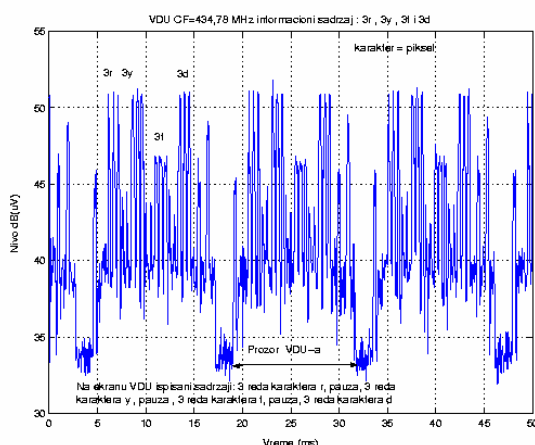
На Дијаграмима 1, 2, 3 и 4 приказан је садржај циљног VDU-а у временској домени (претраживања и одређивање дискриминационих обележја су вршена у фреквенцијској домени, а приказ резултата је дат у временској домени).

На дијаграму 1 је приказан спектар радијационих паразитних зрачења у фреквенцијском опсегу од 100 MHz до 600 MHz без садржаја на екрану.



Дијаграм 1.

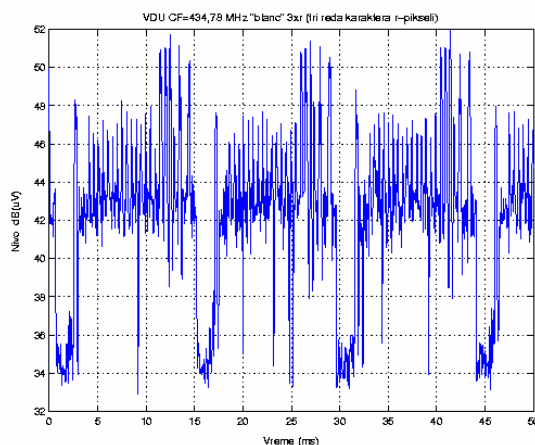
На дијаграму 2 је приказан спектар радијационих паразитних зрачења у фреквенцијском опсегу од 100 MHz до 600 MHz са словним тест сигналом на екрану (3 реда слова **r**, 4 празна реда, 3 реда слова **y**, 4 празна реда, 3 реда слова **t**, 4 празна реда и 3 реда слова **d**).



Дијаграм 2.

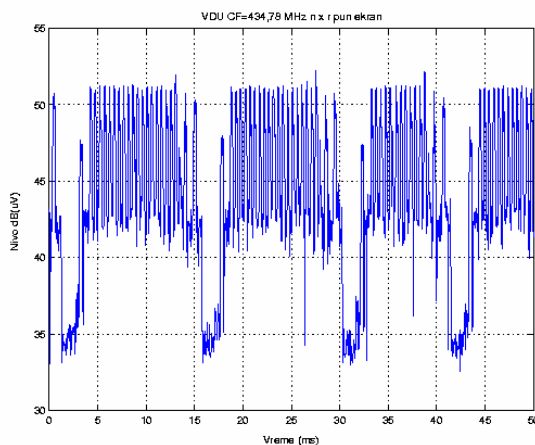
На дијаграму 3 је приказан спектар радијационих паразитних зрачења у фреквенцијском опсегу од 100 MHz до

600 MHz са словним тест сигналом на екрану (21 празан ред и 3 реда слова **r**).



Дијаграм 3.

На дијаграму 4 је приказан спектар радијационих паразитних зрачења у фреквенцијском опсегу од 200 MHz до 600 MHz са словним тест сигналом на екрану: **n** редова слова **r**.



Дијаграм 4.

Друга група експеримената обављена је у циљу одређивања максималне удаљености детекције КЕМЗ и реконструкције слике екрана рачунара. Циљни рачунар се налазио у фабричкој хали (постављен на колица), а у његовој близини је радио други ПЦ. Стандардне пасивне пријемне антене: биконусна (за фреквенцијски опсег од 20 до 200 MHz) и лог-периодична (за фреквенцијски опсег од 80 до 1000 MHz) су прво постављане ван фабричке хале на удаљеност од 10м, а затим је sukcesивно повећавано растојање на 25, 30 и 40м. Треба истаћи да се на удаљеностима већим од од 20м између пријемне антене и фабричке хале (у којој је био циљни рачунар)

налазила метална ограда. Максимална удаљеност узмеђу пријемне антене и циљног ПЦ рачунара у овим условима мерења је била 150м.

На сликама бр. 1 до 3 дат је приказ реконструисаних садржаја (радијационог КЕМЗ-а) са екрана циљног ПЦ рачунара на монитору мерног система, при том циљни ПЦ није предходно испитан у фарадејевом кавезу у циљу одређивања фреквенција најизраженијег нивоа КЕМЗ. Мерења су вршена на предметним растојањима напред наведеним.

Реконструисане слике су јасне и у потпуности читљиве.



Слика бр.1: Реконструисани садржај екрана рачунара на основу радијационог компромићујућег ЕМ зрачења.



Слика бр.2: Реконструисани садржај екрана рачунара на основу радијационог компромићујућег ЕМ зрачења.



Слика бр.3: Реконструисани садржај екрана рачунара на основу радијационог компромићујућег ЕМ зрачења.

Треба истаћи да електромагнетска околина у којој је ово рађено одговара индустријској зони са многобројним изворима паразитних електромагнетских зрачења (радиодифузни предајници и други технички системи у окружењу). Стога се у највећем броју случајева морало радити са атенуацијом улазног сигнала, тј. са пријемником који није у режиму максималне осетљивости.

На слици бр.4 приказан је квалитет реконструисане слике на основу кондукционог компромићујућег ЕМ зрачења постигнутог помоћу струјне сонде постављене око једног од телефонских каблова у амбијенту мерења, када се тест слика састоји од 4 реда слова **W**, 4 празна реда, 4 реда слова **I**, 4 празна реда и 3 реда слова **E**.



Слика бр.4: Реконструисани садржај екрана рачунара на основу кондукционог компромићујућег ЕМ зрачења .

Аналогни експерименти реконструкције слике екрана поновљени су са *notebook* ПЦ, који показују јасан и читљив реконструисани садржај (словни тест сигнал) са екрана овог типа ПЦ рачунара.

Ради илустрације могуће даљине детекције Компромитујућег ЕМ Зрачења, за случај мерења ПЦ (Дијаграми бр.1 до 4) и грубе процене растојања на којем ниво Компромитујућег ЕМ Зрачења опадне на још увек детектабилни ниво од $1\mu\text{V}/\text{m}/\text{MHz}$, уз коришћење Програма [1] за предвиђање максималне удаљености радијационе детекције КЕМЗ, када су мерења на предметном ПЦ обављена на 1м у Фарадејевом кавезу, израчунато растојање је 250м [2].

9. ЗАКЉУЧАК

- 1) Видео јединице или терминали генеришу електромагнетно поље на фреквенцијама до UHF опсега који садржи хармонике видео сигнала.
- 2) Практично је потврђена могућност даљинске екстракције информација са ПЦ (VDU-a) путем Компромитујућег ЕМ зрачења, тј. могућа је реконструкција слике екрана (VDU) ПЦ рачунара на релативно великим растојањима или на проводницима који пролазе у њиховој близини, посебно када се знају карактеристике самог рачунара, видео картице, монитора и њихових *компромитујућих ем зрачења*.
- 3) Са адекватном опремом у зависности од типа VDU-a или терминала успешно прислушкивање (реконструкција поверљивих или приватних информација) може се извршити до дистанце од **1 км** (уз употребу *специјално пројектованих антена*).
- 4) Евидентна је стална опасност од **злоупотреба** података добијених путем КЕМЗ-а, на ПЦ рачунарима на којима није извршена заштита од отицања података који се обрађују на истим.

ЛИТЕРАТУРА

- [1] Лучић Б.: Програми за предвиђање и одређивање максималне удаљености детекције компромитујућег ЕМ зрачења, када су мерења на предметном ПЦ обављена на 1м у ФК; ТОЦ Београд, 2000.
- [2] Лучић Б.: Резултати мерења на различитим типовима VDU-a; ТОЦ Београд, 1994-2003.
- [3] Лучић Б., Јовановић Б.: Зборник радова научно-стручног скупа на тему: Испитивање квалитета средстава НВО и техничких производа, методе мерења и метролошко обезбеђење.; Београд, децембар 2003.године, Дом ваздухопловства Земун.
- [4] Harold J Highlan.: The Tempest over Leaking Computers, ABACUS.
- [5] W. van Eck, J. Neessen and P. Rijdsdijk: ON THE CHARACTERISTICS OF THE ELECTROMAGNETIC FIELD GENERATED BY VIDEO DISPLAY UNITS.