Jerzy F. KOŁODZIEJSKI[1], Ireneusz KUBIAK[2], Jan M. ŁYSKO[1]

Instytut Technologii Elektronowej (1), Wojskowy Instytut Łączności (2)

doi:10.15199/48.2015.11.11

Narażenia sprzętu elektronicznego promieniowaniem elektromagnetycznym – sposoby generacji i metody ochrony

Streszczenie. *W pracy przedstawiono przyczyny zainteresowania kwestią narażeń sprzętu elektronicznego promieniowaniem elektromagnetycznym. Podano przykłady generatorów impulsowych pól elektromagnetycznych dla celów wojskowych. Szerzej omówiono metody ochrony sprzętu elektronicznego przed oddziaływaniem pól elektromagnetycznych. Zwrócono uwagę na wymagane wyposażenie do prowadzenia badań laboratoryjnych odporności sprzętu elektronicznego na oddziaływanie pól elektromagnetycznych.*

Abstract. *The reasons of interest in problems of electromagnetic radiation threat of electronic systems are given. Some examples of pulse electromagnetic fields generators for military purposes are presented. The methods of protection of electronic equipment and systems against electromagnetic radiation are reviewed.. Remarks on requirements of laboratory testing of electronic systems immunity against electromagnetic radiation are also quoted..* ***(Electromagnetic radiation threat of electronic equipment - methods of generation and protection means).***

Słowa kluczowe: promieniowanie elektromagnetyczne, generator pola elektromagnetycznego, odporność na narażenia elektromagnetyczne.
Keywords: electromagnetic radiation, electromagnetic field generator, immunity to electromagnetic exposure.

Wstęp

W okresie ostatnich kilku-kilkunastu lat kwestia odporności różnych układów, urządzeń i systemów elektronicznych na promieniowanie elektromagnetyczne (EM) w zakresie mikrofalowym (fale centymetrowe i milimetrowe) nabrała dużego znaczenia. Energia przenoszona przez wiązkę promieniowania EM może bowiem wywołać uszkodzenie lub wręcz zniszczenie wrażliwych podzespołów i obwodów elektrycznych, doprowadzając do utracenia funkcji przez „oświetlony" (atakowany) obiekt. Następuje to wskutek indukowania dużych chwilowych napięć i prądów oraz lokalnego wzrostu temperatury w obwodach elektrycznych i przewodnikach. Energia promieniowania elektromagnetycznego może również stanowić zagrożenie dla personelu obsługującego urządzenia. Zgodnie z powszechnie stosowaną normą PN-EN 55024, dopuszczalna wartość natężenia pola to zaledwie 3 V/m. Należy ją uznać jako bardzo małą w porównaniu do pól elektromagnetycznych, na które powinien być odporny sprzęt wojskowy, w obliczu zagrożenia stwarzanego przez tzw broń mikrofalową, p. np. [1]. W tym przypadku normatywne natężenia pola EM, w zależności od rodzaju badanego urządzenia i miejsca jego eksploatacji, wynoszą od 10 V/m aż do 200 V/m, przy czym dotyczy to pól ciągłych, a nie impulsowych. Wymagania związane z odpornością sprzętu elektrycznego i elektronicznego na pola impulsowe zawarte są w wielu dokumentach normalizacyjnych. Przykładem może być norma obronna NO-06-A200:2012 [10]. Zawarte w niej wymagania obejmują oddziaływanie impulsu elektromagnetycznego (do 50 kV/m), jednakże o częstotliwościach dużo mniejszych niż te, z którymi mamy do czynienia w przypadku nabierającej coraz większego znaczenia broni mikrofalowej. Ze względu na wymagane bardzo duże natężenia pola elektromagnetycznego, rzędu kilkudziesięciu kV/m i duże częstotliwości sygnałów testowych o wartościach sięgających dziesiątek a nawet setek GHz, badania odporności urządzeń elektronicznych na impulsowe pola elektromagnetyczne stanowią obecnie znaczące wyzwanie techniczne.

Przykładowe rozwiązania generatorów impulsowych pól elektromagnetycznych

Obecne technologie pozwalają na wytworzenie generatorów niszczącego promieniowania EM o zasięgu do kilkunastu kilometrów, typowo ok. 1 km, a w przypadku prostszych rozwiązań o mniejszej mocy („walizkowych") - do kilkudziesięciu metrów. Ze względu na wytwarzanie pola kierunkowego, broń mikrofalowa jest niezwykle precyzyjna i razi cel z dużą dokładnością. Energię wiązki EM uzyskuje się ze źródeł elektrycznych lub chemicznych.

Fotografie poniżej przedstawiają przewoźny generator promieniowania na samochodzie typu Humvee (Hummer) (rys.1) oraz generator przenośny (walizkowy) (rys. 2) - jako jedne z wielu dostępnych obecnie produktów. Podobne rozwiązanie jest także w posiadaniu armii chińskiej (rys. 3).

Rys.1. Przewoźny generator promieniowania na samochodzie typu Humvee – amerykańska broń mikrofalowa Active Denial System ADS (źródło: Wikimedia Commons)

Kierowany strumień energii EM jest wykorzystywany przede wszystkim do celów wojskowych jako broń elektroniczna, choć generatory takiego promieniowania mogą się też, niestety, znaleźć w dyspozycji grup terrorystycznych (sabotażowych).
Zagrożenie – poza urządzeniami i systemami wojskowymi – może więc objąć wiele składników krytycznej infrastruktury narodowej, jak systemy telekomunikacyjne, stacje radiowe i

telewizyjne, sieci energetyczne, systemy sterowania ruchem samochodowym i kolejowym, systemy bankowe, sieci komputerowe itd. Jeśli weźmiemy pod uwagę możliwość ataków terrorystycznych, to trzeba jeszcze uwzględnić kwestie bezpieczeństwa różnorodnych urządzeń stosowanych do automatyzacji procesów produkcyjnych oraz do sterowania i kontroli prowadzonych w ramach różnych form działalności zbiorowej. Występujące tu często mikrokontrolery i komputery są urządzeniami wrażliwymi na oddziaływanie energii promieniowania EM. Jak wspomniano, niektóre z podanych ważnych składników krytycznej infrastruktury narodowej mogą być obiektem ataków terrorystycznych. W przypadku takich działań należy dodatkowo uwzględnić możliwość dostarczenia źródła (generatora) promieniowania EM w pobliże atakowanego obiektu. Natężenie pola elektrycznego w miejscu zlokalizowania celu można wyznaczyć korzystając z przybliżonego wyrażenia [2]

$$E = \frac{\sqrt{30PD}}{r}, \quad (1)$$

w którym: P – moc generatora, D – zysk kierunkowy anteny, r – odległość celu od generatora (źródła) promieniowania. Przy założeniu P =1 kW, D = 8750 i odległości r = 100 m, otrzymuje się natężenia pola o wartości 162 V/m.

Rys.2. Generator przenośny typu DS-110 [2]

Rys.3. Broń mikrofalowa armii chińskiej zaprezentowana podczas wystawy Airshow China 2014 (źródło: http://www.tylkonauka.pl)

Zwróćmy uwagę na jeszcze jeden bardzo ważny aspekt związany z bronią mikrofalową. Otóż, może być ona wykorzystywana nie tylko do obezwładniania lub niszczenia infrastruktury informatycznej przeciwnika. Może być ona również użyta przeciwko personelowi obsługującemu. Skierowanie wiązki promieniującej na ludzi może wywoływać u atakowanego człowieka wrażenie silnego poparzenia i bólu. Jest to skutkiem nagrzewania cząsteczek wody znajdujących się pod skórą człowieka.

Widmo częstotliwości stosowanych sygnałów obejmuje fale radiowe (RF) w zakresie 3 kHz do 300 GHz, przy czym najczęściej są to mikrofale o częstotliwościach powyżej 300 MHz do 300 GHz. Stąd też bierze się nazwa „broń mikrofalowa", a stosowane narażenia w formie impulsów o bardzo dużej szczytowej wartości mocy są znane jako mikrofale dużej mocy HPM (od ang. High Power Microwave). Zwykle impulsy zajmują niewielki zakres częstotliwości. Gdy przedział częstotliwości przebiegów zawartych w impulsie jest stosunkowo szeroki np. 0,3 do kilku GHz, to takie narażenie wyróżnia się stosując skrótową nazwę UWB (od ang. Ultra Wide Band). Od częstotliwości przebiegów stanowiących składowe wiązki promieniowania zależy sposób jej penetracji do obwodów elektrycznych w atakowanym urządzeniu oraz szczegółowy mechanizm powodowania degradacji. Szczególnie niekorzystna sytuacja występuje wówczas, gdy wypromieniowana energia zawiera przebiegi o częstotliwościach mieszczących się w pasmach częstotliwości użytkowanych w danym urządzeniu i/lub stanowiących częstotliwości rezonansowe. Jednocześnie trzeba podkreślić, że ostrość narażeń jest tu większa niż w przypadku wyładowań ESD ze względu na większą stromość narastania impulsów.

Urządzeniami najbardziej narażonymi na oddziaływanie silnych, impulsowych pól elektromagnetycznych są urządzenia wyposażone w antenę lub systemy antenowe oraz posiadające przewody zasilające i sygnałowe wprowadzane do wnętrza urządzenia. W każdym z tych elementów, w trakcie oddziaływania zewnętrznego pola elektromagnetycznego, generowane są znacznej wartości napięcia i prądy, mogące „penetrować" układy elektroniczne, powodując ich nieodwracalne uszkodzenia.

Metody zabezpieczania przed oddziaływaniem pól elektromagnetycznych

Skuteczna ochrona sprzętu elektronicznego przed mikrofalowym promieniowaniem EM wymaga zastosowania szeregu ukierunkowanych działań i środków zaradczych już na etapie projektowania i przy wykonawstwie tych urządzeń. Skuteczna ochrona przed kierowaną energią EM musi być więc kompleksowa, przy uwzględnieniu takich operacji i działań jak: ekranowanie sprzętu, absorpcja energii EM i jej odbicie, zastosowanie ograniczników (limiterów) impulsów, zastosowanie filtrów oraz przyjęcie specyficznych rozwiązań układowych, a także wykorzystanie podzespołów i układów elektronicznych o podwyższonej odporności na napięciowe zaburzenia impulsowe.

a) Ekranowanie

Osłona chroniąca wydzielony obszar przed wpływem zewnętrznego pola elektromagnetycznego powinna być wykonana z materiałów o dużej konduktywności (arkusze blach, siatki, szyby np. z zatopioną siatką). Rolą ekranu jest, z kolei, w innej sytuacji tłumienie pola elektromagnetycznego, zapobiegające jego rozprzestrzenianiu się w przestrzeni otaczającej źródło emisji. Dotyczy to także sygnałów emisji ujawniających, skorelowanych z przetwarzaną na danym urządzeniu (źródło emisji) informacją niejawną [4]. Na wartość skuteczności ekranowania SE wpływają zarówno odbicia jak i absorpcja energii fal pola EM. Zasadniczym elementem ekranowania jest zwykle obudowa urządzenia (rys.4) [4].

Rys.4. Przykład obudowy ekranującej chroniącej znajdujące się w niej urządzenie przed oddziaływaniem zewnętrznego pola elektromagnetycznego oraz przed wypromieniowywaniem znacznej energii elektromagnetycznej w otaczającą przestrzeń (podczas pracy pokrywa jest oczywiście zamknięta)

Zapewnienie skutecznego, a więc ciągłego i mającego właściwe uziemienie, ekranowania obejmuje również przewody i kable połączeniowe oraz różne złącza przewodów i kabli elektrycznych oraz światłowodowych.

b) Absorpcja

Zdolność materiału do pochłaniania energii fali elektromagnetycznej - absorpcja zwiększa się wraz ze wzrostem częstotliwości fali elektromagnetycznej, grubości ekranu, przenikalności magnetycznej ekranu i przewodności. Straty przy pochłanianiu są proporcjonalne do grubości ekranu i jego współczynnika pochłaniania.
Materiał absorbujący tłumi energię mikrofal wskutek strat dielektrycznych, powodujących absorpcję składowej elektrycznej pola np. na cząsteczkach węgla, wprowadzonych do bazowego elastomeru. Z kolei, za absorpcję składowej magnetycznej odpowiadają straty magnetyczne wywołane przez wypełniacze magnetyczne takie jak proszki żelaza i ferryty. Materiały absorpcyjne wytwarza się w formie arkuszy o grubości rzędu części milimetra do kilku milimetrów lub jako materiały piankowe. Instaluje się je na drodze wiązki promieniowania mikrofalowego lub pokrywa się nimi wnęki mikrofalowe [5]. Wśród najnowszych rozwiązań absorberów bierze się także pod uwagę nanorurki węglowe CNT i grafen, przydatny w strukturach płaskich [6].

c) Ograniczniki (limitery)

Tradycyjnymi podzespołami ograniczającymi wartości szczytowe napięcia w obwodach elektrycznych spowodowane przez wyładowania ESD i wyładowania atmosferyczne są: gazowe lampy wyładowcze GDT, przerwy powietrzne, diody p-n (znane jako elementy ograniczające TVS), diody Schottky'ego i PIN, warystory, tyrystory oraz elementy ferrytowe (w falowodach lub na przewodach), [7]. W przypadku impulsowych pól EM jako ochronę czołową stosuje się ponadto ograniczniki plazmowe – z wyładowaniem plazmowym w gazie, [8]. Przyjmuje się, że skuteczne ograniczenie impulsów napięciowych zapewnić może na ogół dopiero dwustopniowa kombinacja odpowiednio dobranych podzespołów ograniczających [9].

d) Filtry

Stosowane są w obwodach zasilania oraz w sieciach sygnałów użytecznych i sterujących. Skuteczność filtracji osiągana jest przy jej kompleksowym stosowaniu wraz z ekranowaniem, wobec źródła emisji lub źródła poddawanego oddziaływaniu zewnętrznego pola elektromagnetycznego. Wówczas filtry muszą być montowane na granicy obszarów ekranowanych.

Stosowanie filtrów w obwodach zasilania, jak i w obwodach sygnałowych, powinno spełniać jeszcze dodatkowo jedną ważną rolę. W przypadku urządzeń przetwarzających informacje niejawne, filtry muszą odpowiednio tłumić sygnały niepożądane występujące poza pasmem sygnału użytecznego.

e) Specjalizowane rozwiązania układowe

Nie wnikając szczegółowo w specjalizowane rozwiązania układowe, wiążące się z funkcjonalnym przeznaczeniem danego urządzenia, wspomnieć tu należy o zalecanym stosowaniu w krytycznych miejscach obwodów elektrycznych techniki światłowodowej oraz o różnicowej metodzie przesyłania sygnałów LVDS od ang. Low Voltage Differential Signaling). Warto też wspomnieć o potrzebie wykorzystywania w obwodach elektrycznych elementów o podwyższonej odporności na narażenia napięciowe.

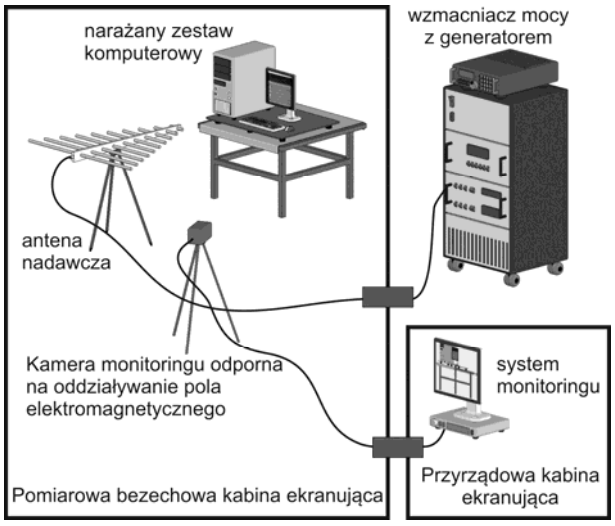
Omawiane tu w wielkim skrócie zagadnienia ochrony sprzętu elektronicznego są przedmiotem prac szeregu grup badawczych w wielu krajach. Znalazły też swe odzwierciedlenie w udzielaniu odpowiednich dotacji (grantów) w ramach NATO i 7-go programu ramowego Unii Europejskiej.

Odporność na ciągłe pole elektromagnetyczne

Celem uświadomienia sobie zagrożeń związanych ze skutkami oddziaływania broni mikrofalowej, spójrzmy na efekty oddziaływania na sprzęt informatyczny (zmodyfikowany pod kątem możliwości przetwarzania informacji niejawnych) ciągłego pola elektromagnetycznego o częstotliwościach do 1 GHz i natężeniu nie przekraczającym 30 V/m [3]. Są to pola o parametrach mniej krytycznych niż występujące w przypadku promieniowania typu HPM. Jednak już i one skutecznie zakłócają pracę urządzeń informatycznych, a w skrajnych przypadkach doprowadzają do ich uszkodzenia. Badania przeprowadzono w układzie przedstawionym na rys. 5. W przypadku zestawu komputerowego oddziaływanie silnych pól elektromagnetycznych powodowało:

- zaburzenia w pracy monitora (rys. 6),
- zakłócenia w pracy myszki i klawiatury;
- losowe uruchamianie zainstalowanych aplikacji;
- przypadkowe kopiowanie i kasowanie plików znajdujących się na dysku.

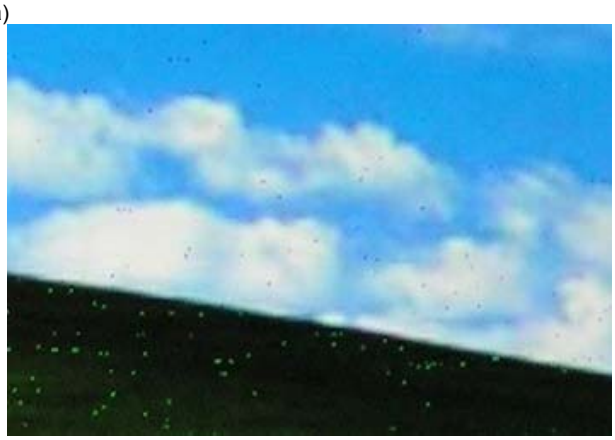
Przy wykorzystaniu pól elektromagnetycznych dużej mocy możliwe jest czasowe unieszkodliwienie (chwilowa niezdolność do pracy), a nawet zniszczenie zestawu komputerowego.



Rys.5. Układ pomiarowy do badań odporności urządzeń na oddziaływanie ciągłego pola elektromagnetycznego dla częstotliwości od 2 MHz do 1 GHz

Laboratoryjne badania sprzętu pod kątem odporności na podane narażenia EM mogą mieć za podstawę normy IEC serii 61000 (z Podkomitetu SC 77C), dotyczące elektromagnetycznych narażeń impulsowych dużej mocy (w tym od wybuchu jądrowego), normy Unii Telekomunikacyjnej ITU-T i IEEE oraz normy wojskowe – amerykańskie (zwłaszcza MIL-STD-461F) oraz brytyjskie i NATO.

a)



b)

Rys.6. Przykład zakłóconej pracy zestawu monitora komputerowego (LCD) w wyniku oddziaływania pola elektromagnetycznego o natężeniu: a) 10 V/m i b) 20 V/m

Nie można zapominać o polskich Normach Obronnych takich jak NO-06-A200:2012 [10], oraz NO-06-A500:2012 [11], bazujących na normie amerykańskiej MIL-STD-461F.

Wymagania dotyczące wyposażenia laboratoryjnego nie są łatwe do spełnienia, biorąc pod uwagę górne częstotliwości fal dochodzące do kilkudziesięciu GHz i więcej oraz wysokie natężenia pola elektrycznego w komorach bezodbiciowych lub rewerberacyjnych. Komory takie muszą zapewnić odpowiednie tłumienie generowanego pola elektromagnetycznego dla bardzo wysokich częstotliwości. Modelowanie zjawisk i symulacja zachowania się sprzętu elektronicznego przy tego rodzaju narażeniach nie są jeszcze wystarczająco opracowane.

Podsumowanie

Ze względów bezpieczeństwa, urządzenia pracujące w sprzęcie wojskowym i w różnych systemach krytycznej infrastruktury narodowej powinny mieć wystarczającą odporność na impulsowe pola elektromagnetyczne dużej mocy. Wytwarzanie takich pól jest obecnie możliwe na znaczną odległość za pomocą mobilnych systemów generacyjnych. Aby uniknąć zagrożeń konieczne jest zatem szersze uwzględnienie w projektach skutecznej ochrony urządzeń i systemów elektronicznych od promieniowania elektromagnetycznego oraz prowadzenie odpowiednich badań laboratoryjnych odporności.

LITERATURA

[1] FIRE-AT-WILL Uzbrojenie i wyposażenie: Broń mikrofalowa – wstęp i jej mobilne systemy lądowe 14/02/2012, 1-3.

[2] Palisek L., Directed Energy Weapons In Modern Battlefield, *Advance in Military Technology* vol.4, No 2, Dec. 2009

[3] Kubiak I., Musiał S., Terroryzm elektromagnetyczny - nowe zagrożenie współczesnego świata*, Zeszyty Naukowe AON,* 4/2009

[4] Kubiak I., Musiał S., Ochrona informacji a bezpieczeństwo danych i urządzeń w obecności narażeń elektromagnetycznych*, Przegląd Telekomunikacyjny, Wiadomości Telekomunikacyjne,* 6/2013, 486-489

[5] Gear J.T., Microwave absorbers manage military electronics RF interference, www.rfdesign.com August 2004, 6-9

[6] Bhattacharya P., Das CH.K., Kalra S.S., Graphene and MWCNT :Potential Candidate for Microwave Absorbing Materials, *Journ. of Materials Science Research* vol.1, No. 2, April 2012

[7] Nilsson T., Investigation of Limiters for HPM and UWB Front-door Protection, Master thesis Linköping University Nov. 2006

[8] Plasma Sciences Corp., Electromagnetic HPM,UWB and EMP Protection for Mission Critical Shipboard Transducer-Bus Networks, Topic N04-075

[9] Yang G. et al., Cascade protector for Hardening Electronic Devices against High Power Microwave, *Defence Science Journ.* Vol. 59, No. 1 Jan. 2009, 55-57.

[10] Norma Obronna NO-06-A200:2012 Kompatybilność elektromagnetyczna. Dopuszczalne poziomy emisji ubocznych i odporność na narażenia elektromagnetyczne

[11] Norma Obronna NO-06-A500:2012 Kompatybilność elektromagnetyczna. Procedury badań zaburzeń elektromagnetycznych i odporności na narażenia elektromagnetyczne

Autorzy*: prof. dr hab. inż. Jerzy F. Kołodziejski, Instytut Technologii Elektronowej, Al. Lotników 32/46, 02-668 Warszawa, E-mail: jekolo@ite.waw.pl,*
dr inż. Ireneusz Kubiak, Wojskowy Instytut Łączności, ul. Warszawska 22A, 05-130 Zegrze Południowe, E-mail: i.kubiak@wil.waw.pl, dr hab. inż. Jan M. Łysko, Instytut Technologii Elektronowej Oddział PREDOM, ul. Krakowiaków 53, 02-255 Warszawa. E-mail: jmlysko@ite.waw.pl