Marek DRAS[1], Marek KAŁUSKI[1], Monika SZAFRAŃSKA[2]

Radiotechnika Marketing sp. z o. o. (1), Instytut Łączności – Państwowy Instytut Badawczy (2)

doi:10.15199/48.2015.11.04

Impulsy HPM – zaburzenia i ich oddziaływanie na systemy – zagadnienia podstawowe

Streszczenie. *W artykule przybliżone zostały podstawowe zagadnienia związane z impulsami HPM. Zaprezentowane zostały istotne problemy związane z filtracją i przeciwdziałaniem impulsom HPM. Autorzy zwracają uwagę na konieczność stosowania poza dotychczas stosowanymi zabezpieczeniami urządzeń wojskowych przed narażeniami elektromagnetycznymi takimi jak pioruny, iskrzenia nowych zabezpieczeń przed impulsami HPM. W artykule pokazano, że te nowe zabezpieczenia wymagają o wiele większej odporności i szybkości zadziałania.*

Abstract*. This paper show some basic issues of HPM pulses tasks. Some of certain problems of filtration and neutralization against HPS's were estimated. The authors point out that the addition of new special filters to the existing protection of military equipment (for example against electromagnetic exposures such as lightning, sparks) is needed to give new protection against HPM pulses. Should be taken into account that filters against HPM requires greater immunity and response time. (**HPM pulses – disturbances and systems interaction – basic issues**).*

Słowa kluczowe: impulsy HPM, filtracja HPM, broń elektromagnetyczna, energia skierowana.
Keywords: HPM pulses, HPM filtration, electromagnetic weapon, directed energy.

Wstęp

Technologia HPM (High Power Microwave) jest rozwijana na świecie od ponad 20 lat. Dotychczas wykonano wiele prac badawczych, w szczególności w ramach grantów NATO, których wyniki i wnioski są w znacznej mierze utajnione. Radiotechnika Marketing, jako partner działający przy realizacji grantu NCBiR „Nowe systemy uzbrojenia i obrony w zakresie energii skierowanej", działa na rzecz wdrożenia do praktycznych zastosowań skutecznych metod filtracji i przeciwdziałania skutkom oddziaływania impulsów HPM, koniecznych do rozwoju obrony przed tego typu zaburzeniami. W ramach niniejszego artykułu autorzy pragną wprowadzić zainteresowanych czytelników w istotę zagadnień związanych z tematyką, która w Polsce rozważana jest od niedawna.

Z uwagi na fakt, iż efekty działań impulsów HPM stanowią podstawę „nowoczesnej wojny", autorzy zwracają uwagę na zagrożenia wynikające z oddziaływania HPM na urządzenia elektroniczne. Oddziaływanie to jest ewidentne, niszczące lub zakłócające pracę każdego urządzenia, które znalazło się w zasięgu emisji od źródła HPM. Ponadto, jest wiele rodzajów źródeł narażeń taktycznych HPM, mających różnorakie mechanizmy odziaływania na urządzenia elektroniczne.

Biorąc pod uwagę to, iż źródła HPM są bronią masowego rażenia, niezabijającą, nieselektywną, obosieczną, oddziaływującą na atakujących i atakowanych - nie ma możliwości uchylenia się przed nią. Zasięg działania tej broni jest lokalny, zależny od rodzaju użytego źródła i wynosi np. 1500 m. Zaś ochrona przed HPM jest zagadnieniem powszechnym, dotyczącym wszystkich urządzeń elektronicznych na polu walki i w zastosowaniach przemysłowych oraz cywilnych, niezależnie od ich stopnia skomplikowania.

Autorzy zwracają uwagę, że należy uwzględnić oprócz dotychczas stosowanych zabezpieczeń urządzeń wojskowych przed narażeniami elektromagnetycznymi takimi jak pioruny, iskrzenia również nowe zabezpieczenia przed impulsami HPM. W artykule pokazano, że te nowe zabezpieczenia związane z filtracją wymagają o wiele większej odporności i większej szybkości zadziałania.

W artykule przybliżone również zostały podstawowe zagadnienia związane z impulsami HPM. Celem artykułu jest również przybliżenie odbiorcom istoty problemów związanych filtracją i przeciwdziałaniem impulsom HPM, jakie mogą przeniknąć i oddziaływać na systemy, np. systemy pokładowe pojazdów wojskowych.

Autorzy, bazując na pracach prowadzonych w Radiotechnice Marketing, prezentują również wstępne wyniki badań związanych z odziaływaniem i filtracją impulsów HPM, będące efektem wcześniej realizowanego grantu z tej samej tematyki.

Geneza

Na całym świecie są obecnie rozwijane i wdrażane do zastosowań taktycznych w polu inne sposoby walki niż typowo rozumiana dotychczas wojna. Od wielu lat jednym z kierunków, w którym podążają prace, jest wojna oparta m.in. na atakach z wykorzystaniem energii skierowanej w postaci impulsów elektromagnetycznych. Rozwój tego typu narażeń jest szczególnie interesujący z uwagi na fakt, iż impulsy elektromagnetyczne o wysokiej mocy oddziaływujące destrukcyjnie na elektronikę w urządzeniach wojskowych nie powodują strat w ludziach. Elektronika poddana narażeniu przez takie impulsy staje się niezdolna do działania z powodu uszkodzeń lub poprzez zawieszenie się zainstalowanego oprogramowania.

. Dodatkową cechą takiej broni jest to, że może ona oddziaływać zarówno na pewnym obszarze jak i być ukierunkowaną na ściśle określone obiekty. Ponadto impulsy takie są bardzo krótkie (rzędu nanosekund) a ich prędkość propagacji jest praktycznie równa prędkości światła. Wytworzony impuls elektromagnetyczny skutecznie degraduje lub zakłóca wszelkie systemy łączności i transmisji. Takie działanie, w obecnych czasach, gdy prawie każdy element wyposażenia dowództwa wojskowego powiązany jest z komputerami lub podzespołami elektronicznymi, może prowadzić do całkowitego paraliżu systemu dowodzenia.

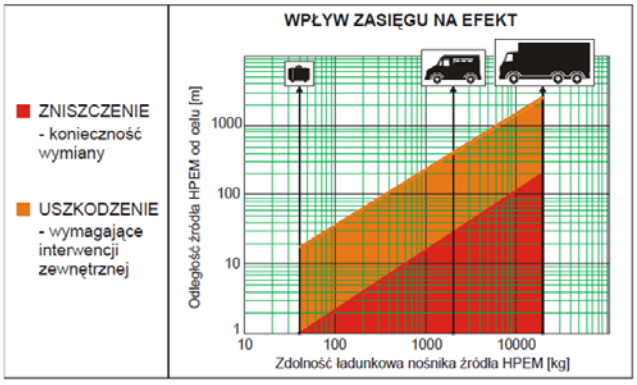
Sam impuls energii skierowanej powoduje wygenerowanie się w poddanych narażeniom układach bardzo silnych prądów, co w efekcie dla większości obecnie stosowanych układów półprzewodnikowych oznacza totalną ich destrukcję, zakłócenie pracy lub zawieszenie się oprogramowania.

Jak wspomniano na wstępie, od ponad 20 lat prowadzone są prace w ramach działań NATO mające na celu zabezpieczanie obiektów przed działaniem broni elektromagnetycznej a w szczególności przed impulsowymi polami elektromagnetycznymi. Przez wiele lat na świecie poniesiono duże nakłady finansowe na badania w zakresie obrony i ochrony urządzeń przed działaniem HPM, uzyskując szereg wyników możliwych do zastosowań praktycznych. W szczególności wyniki kilku grantów NATO-

RTO i NATO-SCI z zakresu HPM stanowią bogate źródło wiedzy (które niestety w dużej mierze jest utajnione) na temat zaobserwowanych przykładów zachowania systemów ochrony przed HPM w sprzęcie wojskowym.

Impulsy HPM

Na rysunku 1, w celu uświadomienia odbiorcom jak potężne impulsy mogą być wytworzone przy stosunkowo mobilnych strukturach, pokazano wykres, na którym uwidoczniono w zależności od wielkości urządzeń generujących impulsy (w kg) i w postaci symbolicznych walizek, furgonetek lub ciężarówek, zaprezentowano ich zasięg działania (w m). Na poniższym rysunku oznaczono kolorami również zakresy, w których urządzenia elektroniczne poddane tym narażeniom albo zostaną uszkodzone (górna część zaznaczonego obszaru – jaśniejsza) albo trwale zniszczone (dolna część zaznaczonego obszaru – ciemniejsza).



Rys.1. Ilustracja zależności rodzaju, wielkości i odległości nośnika na zasięg rażenia

Rys.2. System taktyczny HPM podczas testów (Armia Szwedzka)

Opisując urządzenia generujące zaburzenia elektromagnetyczne należy rozróżnić aparaturę stosowaną do laboratoryjnych badań HPM oraz urządzenia wytwarzające bardzo silne impulsy HPM do celów taktycznych czy terrorystycznych. Aparatura, która może być stosowana w laboratorium do badań odporności urządzeń na zjawiska wywoływane tymi impulsami zazwyczaj wytwarza powtarzalne i regulowane, relatywnie słabe impulsy HPM w sposób ciągły. Duże systemy i urządzenia do celów taktycznych, jak na rysunku 2, wytwarzają bardzo silne nieregulowane impulsy jednorazowe lub w małej ilości z tylko jednym ich przeznaczeniem do niszczenia atakowanych obiektów. Typowo urządzenia takie są zamontowane na pojazdach wojskowych lub na samolotach i mają za zadanie działać jako broń, a nie jako urządzenie, które w sposób powtarzalny może generować zaburzenie. Np. firma Boeing w 10.2013 roku, w ramach programu CHAMP z bezzałogowego samolotu, generując impulsy HPM zniszczyła sieci komputerowe, systemy alarmowania i zasilania w całym kompleksie budynków.

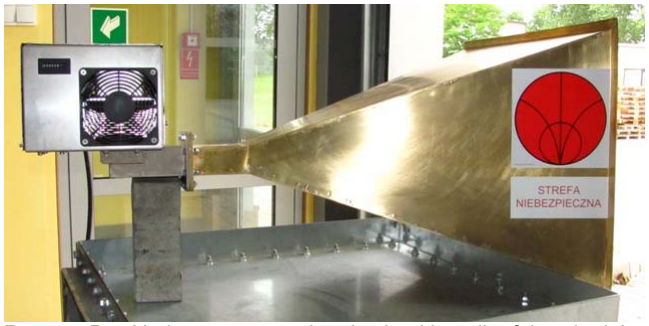
Prezentowany na rysunku 2. układ jest przykładem również na to jak dalece sojusznicy z NATO biorący udział w grantach rozwojowych energii skierowanej są posunięci w rozwiązaniach technologicznych z zakresu HPM.

Dotychczas w Polsce zrealizowany został tylko jeden grant związany z tą tematyką. Na rysunku 3 zaprezentowano walizkowe urządzenie generujące zaburzenia impulsowe o energii 0,2J, które stosowane było podczas realizacji grantu dla MSWiA. W Tablicy 1 podane zostały podstawowe parametry systemu narażeń impulsami Diehl DS110F.

Rys.3. Walizkowy system generacji impulsów Diehl DS110F podczas testów (w ramach grantu MSWiA)

Tablica 1. Parametry generatora Diehl DS110F

Rozmiar	500x410x200 mm3
Masa	24 kg
Moc szczytowa (peak power)	160 MW
Promieniowanie (bez reflektora)	Dipol
Czas trwania impulsu	4 ns
Czas powtórzeń impulsu	>5 Hz (10Hz typ)
Częstotliwość	350 MHz
Szerokość pasma 3 dB	100 MHz
Czas pracy (bez ładowania)	>1 godz

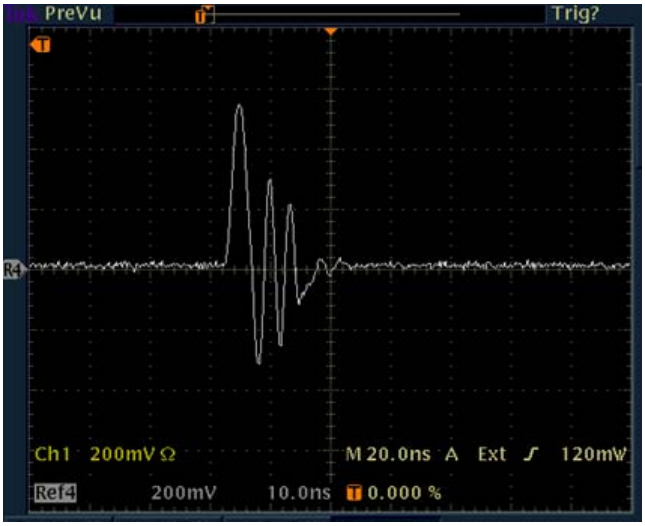


Rys.4. Przykład zastosowania kuchenki mikrofalowej jako mikrofalowego źródła mocy

Kolejnym przykładem zastosowania broni impulsowej narażającej polem elektromagnetycznym jest stosunkowo łatwa w konstrukcji broń terrorystycznego zastosowania w postaci odpowiednio zmodyfikowanej kuchenki mikrofalowej. Poprzez wykorzystanie wbudowanego źródła (magnetronu) w kuchenkach mikrofalowych i ukształtowanie wiązki anteną np. tubową możemy uzyskać źródło, które będzie miało ponad 2 kW mocy. Teoretycznie moc ta nie

jest na tyle duża aby można powiedzieć że jest to znaczące źródło, jednakże ze względu na znaczną energię i ukierunkowanie jest ona wystarczająca na przykład do zdezorganizowania łączności w paśmie 2,4 GHz na obszarze nawet kilkuset metrów. Na rysunku 4 pokazano przykład przebudowanej kuchenki mikrofalowej do narażeń terrorystycznych.

Należy pamiętać, że ze względu na różne rodzaje i charakter impulsów HPM stosowanych przez potencjalnego atakującego, każdy z nich ma inne własności zakłócające lub niszczące przy oddziaływaniu na narażane urządzenia lub ich obwody. Dlatego też chcąc przygotowywać zabezpieczenia przed różnego rodzaju impulsami należy wyposażyć się w odpowiednią aparaturę laboratoryjną lub dostosować już posiadaną aparaturę wytwarzającą narażenia HPM, tak aby możliwie szeroko pokryć spektrum i złożoność występujących w rzeczywistości narażeń HPM. W ramach prac własnych będących przygotowaniem Radiotechniki Marketing do realizacji grantu NCBiR „Nowe systemy uzbrojenia i obrony w zakresie energii skierowanej" przygotowano specjalne stanowisko umożliwiające wytarzanie różnorodnych impulsów HPM zarówno w postaci fal radiowych ciągłych jak i bardzo silnych impulsów HPM. Jak wspomniano wyżej, urządzenia laboratoryjne nie mają za zadanie wytworzenia wielomegawatowych impulsów, ale ich zadaniem jest generowanie powtarzalnych sygnałów o zbliżonym charakterze (kształt, sposób generowania/oscylacji).



Rys.5. Impuls wygenerowany w laboratorium Radiotechniki Marketing

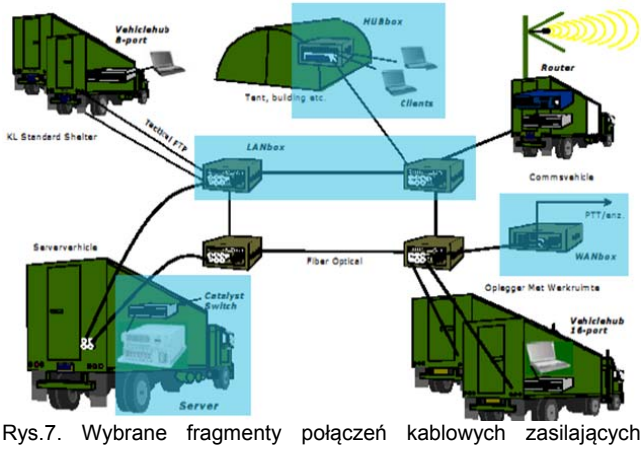
Rys.6. Stanowisko, na którym generowany był impuls jak na rys. 5

Przykład stanowiska oraz impuls, jaki został wygenerowany na tym stanowisku zaprezentowano na rysunkach 5 i 6 Impulsy te są stosowane do badań układów filtracyjnych, które będą docelowym rozwiązaniem dla ochrony przed bronią HPM. Symulacja laboratoryjna pozwala na wielokrotne próby badań sposobu przenikania impulsów poprzez zabezpieczenia bez groźby trwałego uszkodzenia urządzeń stosowanych podczas badań.

Sposoby ochrony

Urządzenia ochrony przed HPM to m.in. specjalne kable i okablowanie do zasilania i transmisji, układy zasilania, połączenia światłowodowe oraz przyłącza zasilania i sterowania a w szczególności filtry zapewniające odpowiednie separowanie. Wszystkie te powszechnie spotykane urządzenia ze względu na swoja budowę, sposób działania i stosowania na otwartych przestrzeniach, są najbardziej podatne na oddziaływanie impulsów HPM. Bardzo często, gdy wiązki/przewody prowadzone są pomiędzy odległymi punktami, działają one, jako naturalne długie rozciągnięte po ziemi anteny odbiorcze tych impulsów i wprowadzają je do wnętrza wszystkich systemów elektronicznych na polu walki. Na rysunku 7 przedstawiono wybrane fragmenty połączeń kablowych zasilających i transmisyjnych między kontenerami typowego taktycznego stanowiska dowodzenia systemów wojskowych C4I, które były poddane badaniom w ramach grantu NATO RTO SCI-132. Badaniom poddano również sprzęt aktywny dołączony do takich kabli. Stąd też budowa w/w systemów i urządzeń zabezpieczonych przed HPM jest niejako budową pierwszej linii obrony dla wszystkich systemów wojskowych zawierających urządzenia elektroniczne. Świadczy to nie tylko o potrzebie zabezpieczania układów elektroniki wejścia/wyjścia, ale również o konieczności stosowania odpowiednich zabezpieczeń (w szczególności ekranowania) już na poziomie przewodów czy wiązek kablowych łączących potencjalnie wrażliwe elementy.

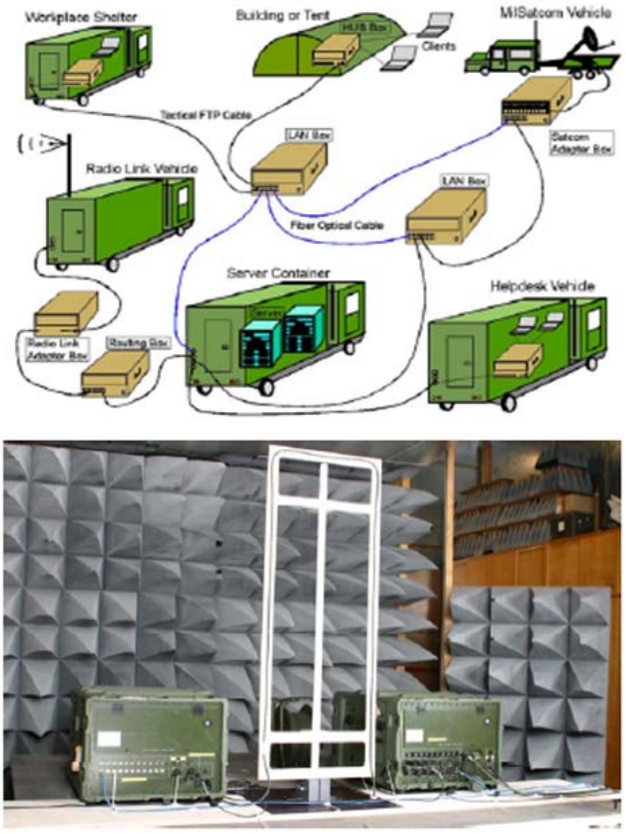
Należy również wspomnieć, że z wyników wykonanego przez RM grantu rozwojowego wynika, że metoda bazująca na samym ekranowaniu kabli w typowy sposób jest niewystarczająca do zabezpieczenia przed impulsami HPM. Stosowanie ekranów wielowarstwowych powoduje takie usztywnienie kabli, że nie nadają się praktycznie do rozwijania i zwijania. Dlatego też należy zwrócić uwagę na potrzebę zaprojektowania, zbudowania i przetestowania kabli o innych strukturach wewnętrznych uniemożliwiających przewodzenie i rozchodzenie się w nich sygnałów wywoływanych przez HPM i niszczących dołączone układy elektroniczne.



Rys.7. Wybrane fragmenty połączeń kablowych zasilających i transmisyjnych między kontenerami typowego taktycznego stanowiska dowodzenia C4I (źródło prezentacja Fraunhofer)

Ponadto połączenia kablowe dołączone są do urządzeń wojskowych poprzez układy wejściowo-wyjściowe. Są one wykonywane, jako tablice przyłączy zewnętrznych zasilania, komunikacji i sterowania. Takie tablice muszą stanowić zabezpieczającą barierę ochronną wejściową przed niszczącymi sygnałami przychodzącymi z wszystkich dołączonych do tych urządzeń różnorodnych kabli poddanych narażeniom HPM. Tablice przyłączeniowe muszą ponadto równocześnie spełniać inne funkcje np. filtracji zakłóceń, załączania i wyłączania zasilania, co powoduje konieczność rozbudowy systemu zabezpieczeń przed HPM. Dlatego tak istotne jest, aby poprzez odpowiednią filtrację i jakość stosowanych przyłączy zapewnić odseparowanie od źródła impulsu HPM.

Wspomnieć należy również o odpowiednio zabezpieczonych przed oddziaływaniem HPM urządzeniach zasilania zmienno- i stałoprądowego, które stanowią podstawowy element działania każdego urządzenia elektrycznego.



Rys.8. Przykład badan połączeń światłowodowych i urządzeń z nimi współpracujących stosowanych na stanowiskach dowodzenia C4I (źródło prezentacja Fraunhofer)

Jak powszechnie wiadomo to układy zasilania będące najbardziej zewnętrznym elementem systemów a także głównym buforem dla nich są najbardziej narażone na działanie wszelkich zaburzeń. Dlatego też zwrócenie szczególnej uwagi na te elementy jest bardzo istotne. Ponadto jak wynika z prac prowadzonych w grancie dla MSWiA oraz z prac NATO-RTO, zasilacze zawierające przetwornice (czyli praktycznie każde) bardzo łatwo się uszkadzają, zarówno od strony wejścia zasilania sieciowego 230 V, jak i od strony wyjścia stałoprądowego 24 V, w chwili poddania ich narażeniu impulsami. Niezawodne systemy zasilające, w tym UPS, są podstawowym i niezbędnym elementem działania jakichkolwiek urządzeń elektronicznych a zwłaszcza wojskowych.

Nieco zaskakującym może okazać się potrzeba zabezpieczenia przed oddziaływaniem HPM przyłączy światłowodowych, ponieważ same światłowody są teoretycznie odporne na oddziaływanie fal elektromagnetycznych. Jest to częściowo prawda. Same światłowody są odporne, ale wraz z przyłączami, złączami światłowodowymi i dołączonym konwerterem systemy światłowodowe są wg badań dokonanych w NOTO-RTO najbardziej podatnym na narażenia HPM elementem polowym sieci komputerowych systemów C41. Ta informacja była utrzymywana w tajemnicy w NATO przez kilka lat, a jest bardzo ważna dla bezpieczeństwa działania systemów transmisji danych na stanowiskach dowodzenia. Poniżej, na rysunku 8, podano przykład takich badan połączeń światłowodowych i urządzeń z nimi współpracujących stosowanych na stanowiskach dowodzenia C4I.

Podsumowanie

Obecnie w Polsce nie ma generatorów do wytwarzanie impulsów HPM. Generatory do zastosowań badawczych są co prawda urządzeniami o stosunkowo małej mocy i ich oddziaływanie na narażane urządzenia jest stosunkowo słabe, jednak powodują one zakłócenia działania tych urządzeń.

Narażenia, jakim poddawane są urządzenia w badaniach laboratoryjnych, pokazują jak ważna jest odpowiednia filtracja nie tylko poprzez stosowanie typowych rozwiązań, ale wymagających specjalnych opracowań. Należy zwrócić uwagę, że gdyby dysponować odpowiednimi źródłami impulsów HPM efekty oddziaływania mogłyby być nawet 100 razy silniejsze i uzyskiwane z dużych odległości – setek metrów.

LITERATURA

[1] „Opracowanie technologii i demonstratora zabezpieczenia systemów teleinformatycznych służb porządku publicznego w aspekcie narażenia na terrorystyczne działanie silnych impulsów elektromagnetycznych”, opracowanie będące wynikiem grantu rozwojowego NCBiR nr 0R00006311, wykonanego w latach 2010-2012 przez WAT, RM i CTM

[2] publikacje wyników grupy NATO-RTO SCI-132

[3] publikacje wyników grupy NATO-RTO SCI-119

[4] publikacje wyników grupy NATO-RTO SCI-198

[5] Bendord J., Swegle J.A., Schamiloglu E., High Power Microwaves, ISBN 0-7503-0706-4

[6] Kuchta M., Kubacki R., Nowosielski L., Dras M., Wierny K., Namiotko R., Standardy bezpieczeństwa dla urządzeń teleinformatycznych zabezpieczające przed terroryzmem elektromagnetycznym, *Przegląd Elektrotechniczny*, nr 12, 2012

[7] Wierny K., Wpływ impulsów elektromagnetycznych dużej mocy na elementy systemy teleinformatycznego, opracowanie Radiotechnika Marketing sp. z o.o.

[8] Dras M., Odporność wojskowych urządzeń elektronicznych na narażenia elektromagnetyczne o wysokiej energii (HPM), III Konferencja Łączności, Sieradz, marzec 2012

[9] materiały udostępnione przez firmę Diehl BGT Defence

***Autorzy**: mgr inż. Marek Dras, Radiotechnika Marketing Sp. z o. o., ul. Fabryczna 20, Pietrzykowice, 55-080 Kąty Wrocławskie, E-mail: MDras@radiotechnika.com.pl; mgr inż. Marek Kałuski, Radiotechnika Marketing Sp. z o. o., ul. Fabryczna 20, Pietrzykowice, 55-080 Kąty Wrocławskie, E-mail: MKaluski@radiotechnika.com.pl; mgr inż. Monika Szafrańska, Instytut Łączności – Państwowy Instytut Badawczy, Zakład Kompatybilności Elektromagnetycznej, ul. Swojczycka 38, 51-501 Wrocław, E-mail: M.Szafranska@itl.waw.pl.*