Andrzej KACZMAREK[1], Rafał NAMIOTKO[1]

Ośrodek Badawczo-Rozwojowy Centrum Techniki Morskiej S.A. (1)

Szacowanie progów podatności urządzeń infrastruktury krytycznej na oddziaływanie impulsowego pola elektromagnetycznego dużej mocy

Streszczenie. *W referacie omówiono przykładowe metody narażeń (ataków) polem elektromagnetycznym na urządzenia infrastruktury krytycznej. Zaprezentowano skutki oddziaływania impulsów dużej mocy (HPEM) na urządzenia telekomunikacyjne i teleinformatyczne. Przedstawiono metodę szacowania progów podatności infrastruktury krytycznej oddziaływania impulsowego pola elektromagnetycznego.*

Abstract*. The paper described the methods exposed sample (attacks) on the electromagnetic field of critical infrastructure equipment. Presented the effects of high-power pulses (HPEM) for telecommunication and data communication equipment. The paper showed a method for estimating the vulnerability of critical infrastructure limits the impact of pulsed electromagnetic field. (**Estimating the sensitivity thresholds for critical infrastructure installations to the effects of high power pulsed electromagnetic field**).*

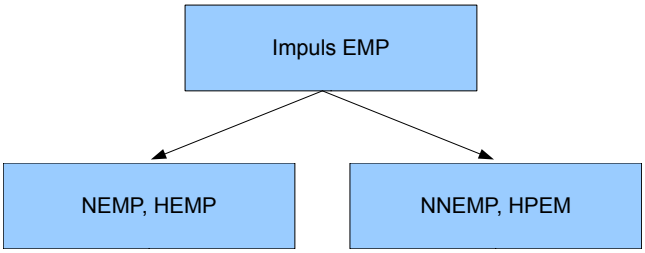
Słowa kluczowe: pole elektromagnetyczne, infrastruktura krytyczna, impulsy dużej mocy, progi podatności.
Keywords: electromagnetic field, critical infrastructure, high-power pulses, sensitivity thresholds.

doi:10.12915/pe.2014.07.37

Wstęp

Infrastruktura krytyczna jest narażona na wszelkiego rodzaju ataki ze strony nie powołanych osób, oprócz ataków hakerów czyli wtargnięcia do systemu poprzez środowisko programistyczne, możliwe jest wyłączenie, zakłócenie pracy, a nawet zniszczenie przetwarzanych danych oraz urządzeń telekomunikacyjnych, teleinformatycznych poprzez wygenerowanie w ich pobliżu silnego impulsu elektromagnetycznego dużej mocy.

Metody narażenia polem elektromagnetycznym możemy podzielić ze względu na wytworzenie impulsu na generowane z wybuchu jądrowego oraz generowane poprzez ładunki wybuchowe lub poprzez specjalnie skonstruowane układy elektroniczne.

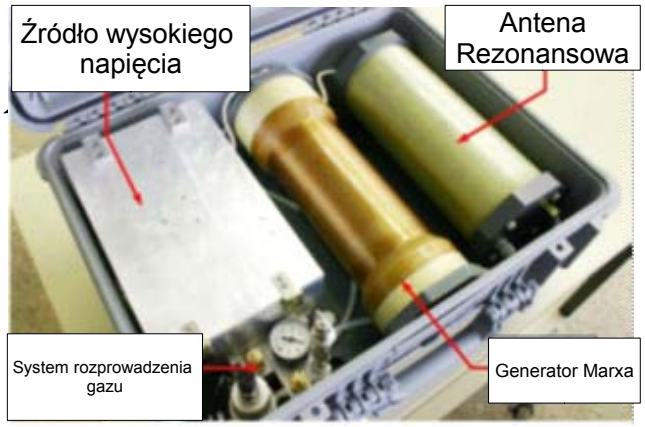


Rys.1. Podział impulsów EMP

Impulsy generowane za pomocą wybuchu jądrowego są to impulsy NEMP (Nuclear Electromagnetic Pulse) – impuls wygenerowany po wybuchu bomby atomowej, oraz HEMP (High-Altitude Electromagnetic Pulse) – impuls wygenerowany po wybuchu bomby atomowej na dużej wysokości. Impulsy nie wywołane wybuchem jądrowym są to impulsy NNEMP (Non-nuclera Electromagnetic Pulse) – impuls wywołany konwencjonalnym ładunkiem wybuchowym, wykorzystujący energię elektrochemiczną HPEM (High Power Electromagnetic) – impulsy wytwarzane poprzez specjalnie skonstruowane układy elektroniczne, zbudowane w oparciu o generatora Marxa.

Przykładem generatora HPEM jest generator DS110F (rysunek 2). Jest to małe kompaktowe źródło RF dużej mocy, nadające się do zakłócania urządzeń infrastruktury krytycznej. Kompaktowy, autonomiczny generator HPEM DS110F nadaje się do przedstawienia efektów wpływu impulsów wysokich mocy na sprzęt elektroniczny w rzeczywistych warunkach.

Rys.2. Generator HPEM DS110F



Rys.3. Elementy składowe generatora HPEM System DS110F

Podstawową specyfikację generatora HPEM DS110F przedstawiono w tabeli 1.

Walizka wraz z głównymi częściami generatora HPEM DS110F została przedstawiona na rysunku 3.

Elementami składowymi generatora HPEM są:
- źródło wysokiego napięcia;
- generator Marxa 300 kV;
- antena rezonansowa;
- system rozprowadzania gazu.

Tabela 1. Parametry generatora HPEM System DS110F

Parametr	Wartość
Rozmiar	500x410x200 mm
Waga	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

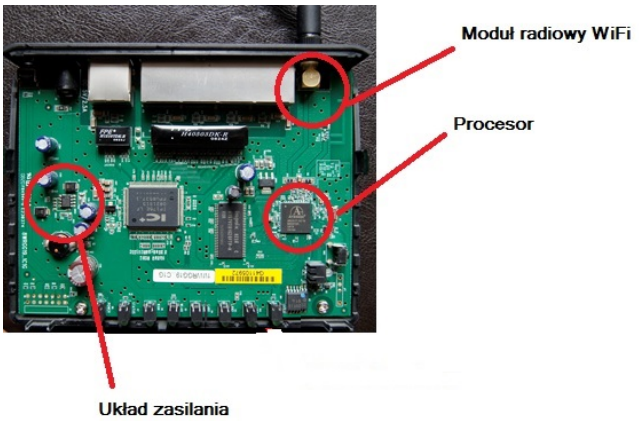
Metoda szacowania progów podatności

Metoda ta polega na przybliżonym określeniu progów podatności urządzeń infrastruktury krytycznej na oddziaływanie impulsowego pola elektromagnetycznego. Metoda szacowania zostanie zaprezentowana na przykładzie określenia progów podatności dla routera standardu 802.11g. Przed przystąpieniem do określania progów podatności należy zapoznać się z właściwościami urządzenia, w tym przypadku mamy do czynienia z bezprzewodowym urządzeniem teleinformatycznym. Im więcej danych zbierzemy na temat elementów składowych i budowy urządzenia tym bardziej dokładnie określimy progi odporności.

Przykładowy router posiada następujące elementy:
- procesor;
- przetwornicę obniżającą napięcie;
- 5 portowy switch;
- układ wejściowy dla WiFi;

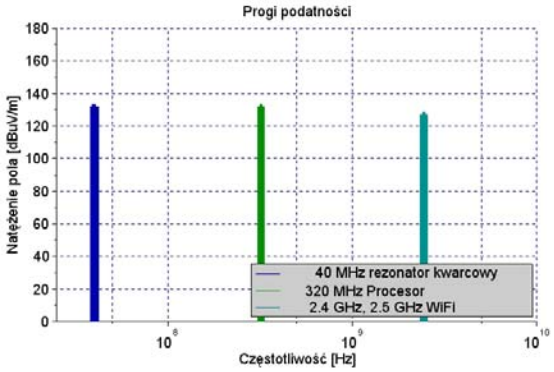
Znając te elementy należy umieścić wszystkie charakterystyczne parametry na wykresie tak jak to przedstawiono na rysunku 5:
- częstotliwość rezonatora kwarcowego 40 MHz, częstotliwość pracy procesora 320 MHz, napięcie pracy od 3 V do 3,6 V;
- układ wejściowy dla WiFi częstotliwość pracy od 2,4 GHz do 2,5 GHz maksymalna moc 15 dBm ± 2 dBm;

Rozmieszczenie elementów elektronicznych urządzenia przedstawiono na rysunku 4.



Rys.4. Elementy składowe routera które mogą wpływać na progi podatności/odporności na oddziaływanie impulsowego pola elektromagnetycznego dużej mocy

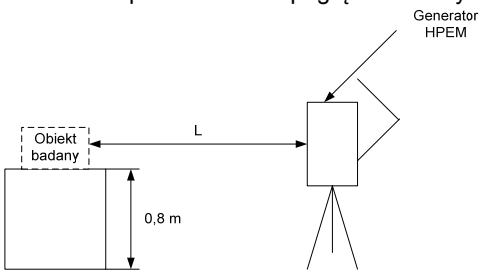
Znając wszystkie elementy które mogą wpływać na progi podatności/odporności rotuera na oddziaływanie impulsowego pola elektromagnetycznego, można przedstawić charakterystyczne punkty na wykresie co przedstawiono na rysunku 5. Wartości napięć pracy rezonatora kwarcowego i procesora oraz maksymalnej mocy pracy układu WiFi przeliczono na jednostki dBμV/m.



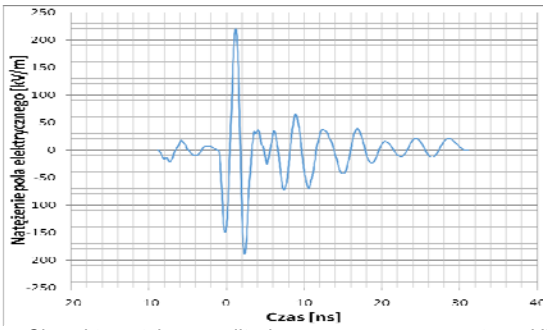
Rys.5. Przedstawienie charakterystycznych elementów routera na wykresie amplitudowo-częstotliwościowym

Badanie oddziaływania impulsów HPEM na elementy infrastruktury krytycznej

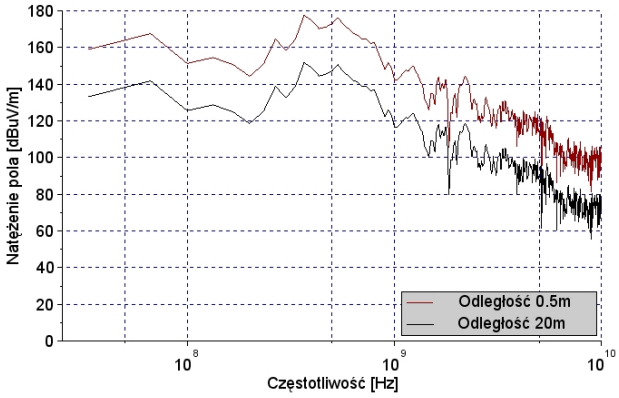
Wykonano stanowisko pomiarowe do badania odporności urządzeń na oddziaływanie impulsów dużej mocy. Stanowisko przedstawiono poglądowo na rysunku 6.



Rys.6. Stanowisko pomiarowe



Rys.7. Charakterystyka amplitudowo-czasowa generatora HPEM pomierzona w odległości 0,5 m od generatora



Rys.8. Charakterystyka amplitudowo-częstotliwościowa generatora HPEM pomierzona w odległości 0,5 m oraz 20 m od generatora

Badanie polegało na sprawdzeniu zachowania się urządzeń w polu impulsowym dużej mocy. Obiekt badany

umieszczony był 0,8 m nad ziemią i oddalony o określoną odległość od generatora HPEM, zmieniając odległość od obiektu badanego zmieniało się natężenie pola generowane z generatora HPEM. Im obiekt badany był dalej od generatora HPEM tym mniejsze zaburzenie generowane przez generator.

Jako obiekt badań wybrano router standardu 802.11g wg rysunku 4 na którym wcześniej wykonano szacowanie progów podatności/odporności. Badanie wykonywano od odległości 20m do 0,5m, co daje natężenie pola w maksymalnym punkcie od 12 kV/m do 220 kV/m. Charakterystykę amplitudowo-czasową generatora HPEM pomierzoną w odległości 0,5m od generatora przedstawiono na rysunku 7, charakterystykę, amplitudowo-częstotliwościową przedstawiono na rysunku 8.

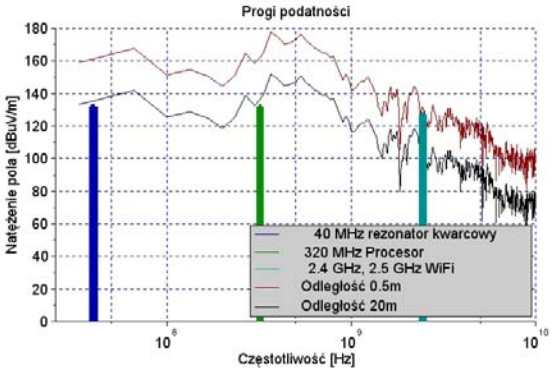
Stanowisko pomiarowe wraz z badanym routerem przedstawiono na rysunku 9.

Rys.9. Stanowisko pomiarowe wraz z obiektem badanym (router WiFi standardu 802.11g)

Wyniki badań

Praca routera standardu 802.11g była sprawdzana programem ping (komputer oddalony o 30 m od routera), przy odległości 17,5 m została zakłócona praca routera. Router resetował się, po zaprzestaniu narażenia jego praca i funkcje powracały do normalnego stanu. Dla odległości 17,5m natężenie pola elektrycznego wynosiło 13 kV/m. Natomiast przy 0,5 m router zawieszał się i był konieczny reset urządzenia poprzez wyłączenie i włączenie ponowne z zasilania.

Charakterystykę amplitudowo-częstotliwościową generatora HPEM wraz z założonymi progami odporności routera przedstawiono na rysunku 10.



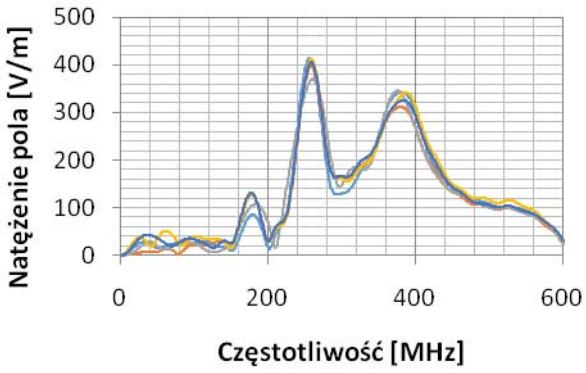
Rys.10. Charakterystyka amplitudowo-częstotliwościowa generatora HPEM wraz z założonymi progami odporności routera.

Zakłócenie się pracy routera (reset routera rozpoczyna się od odległości poniżej 20m), natomiast od 0,5m następuje zawieszenie się routera, wpływ układu WiFi 2,4 GHz – 2,5 GHz widać że dla odległości od 0,5m sygnał z generatora HPEM jest większy niż założony próg odporności.

Zabezpieczenia przed impulsami HPEM

Zabezpieczenia przed oddziaływaniem na impulsy HPEM możemy podzielić ze względu na wnikanie impulsu do urządzenia na:
- wnikanie przez obudowę urządzenia (ekranowanie obudowy);
- wnikanie przez złącza zasilania, transmisji (ekranowanie kabli, filtrowanie).

W celu zabezpieczenia urządzenia przed wnikaniem impulsów HPEM przez obudowę należy zastosować obudowy o odpowiednim tłumieniu fali elektromagnetycznej. Jeżeli impuls HPEM który oddziaływuje na urządzenie ma kształt i amplitudę jak impuls podany na rysunku 11.



Rys.11. Charakterystyka amplitudowa impulsu HPEM

Dla układu o logice 5V można przyjąć że tłumienie obudowy powinno wynosić minimum 40 dB zgodnie ze wzorem 1:

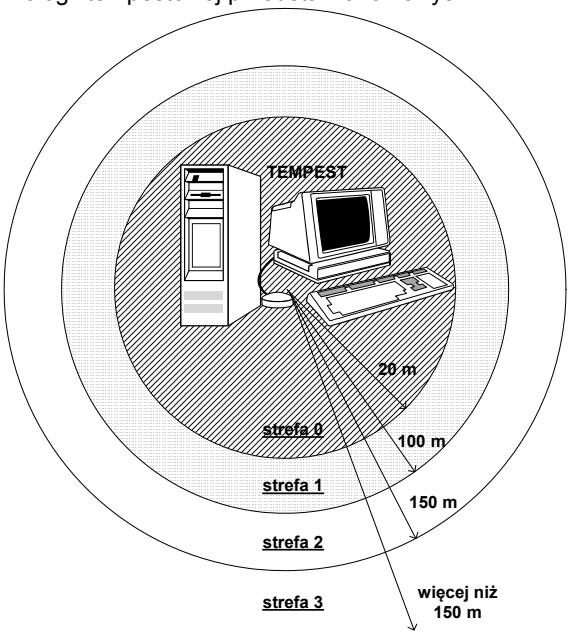
$$SE = 20 * \log 10 \frac{400}{5} \approx 40dB \quad (1)$$

Zabezpieczenie złącza zasilania oraz transmisji urządzenia można wykonać za pomocą odpowiednich elementów włączonych w tor zasilania bądź transmisji. Elementy ochronne muszą tłumić zakłócenia występujące na linii bez zmiany sygnałów użytecznych. Ochrona przeciwko zaburzeniom elektromagnetycznym zazwyczaj polega na zastosowaniu elementów nieliniowych takich jak iskierniki, warystory lub diody. Obwody ochronne powinny być zoptymalizowane i zaprojektowane aby mogły zabezpieczać przed impulsami rzędu nanosekund. Przy ich konstrukcji musi być zawarty kompromis pomiędzy zdolnością pochłaniania energii a szerokością pasma częstotliwości. Szerokie pasmo częstotliwości prowadzi do bardzo niskiej zdolności pochłaniania energii.

Oprócz zastosowania elementów fizycznych w urządzeniu celem zabezpieczenia go przed wnikaniem impulsów HPEM dużej mocy, można zastosować zabezpieczenia systemowe. Jednym z zabezpieczeń systemowych jest ustalenie stref ochronny.

Strefy te wyznacza się na podstawie badania tłumienia pola elektromagnetycznego w przestrzeni miedzy źródłem niepożądanej emisji, a granicą obszaru kontrolowanego, w odległości 20 m, 100 m oraz powyżej 150 m. Przy określaniu takich stref bezpieczeństwa brane są pod uwagę miedzy innymi poziomy tłumienia pola

elektromagnetycznego obiektu budowlanego, lokalizację instalacji energetycznych, informatycznych, telekomunikacyjnych oraz powierzchnię kontrolowanego obszaru. Poglądowy schemat stref bezpieczeństwa i stosowanych w nich urządzeń zwłaszcza wykonanych w technologii tempestowej przedstawiono na rys. 12.



Rys.12. Przykładowe strefy bezpieczeństwa dla urządzeń i systemów

Wyróżnia się następujące strefy bezpieczeństwa oznaczone jako 0, 1, 2, 3:

- 0 – obszar o promieniu < 20 m i/lub odpowiednia skuteczność ekranowania struktury,
- 1 – obszar o promieniu ≥ 20 m oraz < 100 m i/lub odpowiednia skuteczność ekranowania struktury,
- 2 – obszar o promieniu ≥ 100 m oraz < 150 m i/lub odpowiednia skuteczność ekranowania struktury,
- 3 – obszar o promieniu ≥ 150 m i/lub odpowiednia skuteczność ekranowania struktury.

Strefy bezpieczeństwa stosuje się głównie w celu redukcji kosztów wynikających ze stosowania drogich struktur ekranujących o tłumienności rzędu 100 dB. Zastosowanie przykładowo wymogów strefy 1 (obszar powyżej 20 m od urządzenia) oraz struktury ekranującej o tłumienności rzędu 60 dB, daje podobny efekt ekranujący jak zastosowanie dużo droższej w realizacji struktury o tłumienności 100 dB. Wadą podejścia strefowego jest to, że nie wszędzie może mieć ono zastosowanie (np. ochrona w budynkach w centrum miast).

W celu ochrony budynku przed terroryzmem elektromagnetycznym należy wytyczyć strefy bezpieczeństwa dla danego budynku umieszczonego w danej lokalizacji. Wyznaczenie możliwego obszaru ochronnego będzie podstawą do zastosowania określonych środków technicznych o odpowiedniej skuteczności ekranowania dla pola elektromagnetycznego dużej mocy.

Zabezpieczenie przed impulsem dużej mocy HPEM urządzeń transmisji WiFi standardu IEEE 802.11g możliwe było by również poprzez zbudowanie urządzenia opartego na standardzie IEEE 802.21.

Standard IEEE 802.21 opisuje mechanizmy które zapewniają możliwość współpracy warstwy łącza danych z wyższymi warstwami umożliwiając optymalne przełączanie pomiędzy heterogenicznymi mediami. Optymalne przełączanie pomiędzy sieciami heterogeniczynim jest możliwe dzięki umieszczeniu funkcji MIH (ang. Media Independent Handover) pomiędzy warstwą łącza danych a wyższymi warstwami. Informację dostarczane z niższej warstwy poprzez różne technologie przekazywane są do wyższych warstw za pomocą jednego wspólnego interfejsu MIH.

Urządzenie takie byłoby wyposażone w kilka standardów transmisji np. standard WiFi IEEE 802.11, WiMax IEEE 802.16 czy też transmisje 3GPP i w zależności który rodzaj transmisji byłby zakłócany taka transmisja byłaby aktualnie używana do komunikowania się z siecią Internet.

LITERATURA

[1] J. Szóstka Fale i anteny, *WKŁ*, Wydanie 2, Warszawa 2001,

[2] MIL-STD-188-125-1 High-Altitude Electromagnetic Pulse (Hemp) Protection For Fixed Ground-Based C4 I Facilities Performing Critical, 1998,

[3] M.Kuchta, R.Kubacki, L. Nowosielski, M. Dras, K. Wierny, R. Namiotko Standardy Bezpieczeństwa Dla Urządzeń Teleinformatycznych Zabezpieczające Przed Terroryzmem Elektromagnetycznym, Polskie Towarzystow Zastosowań Elektromagnetyzmu, Warszawa 2012 r.

[4] Antonio de la Oliva, Telemaco Melia, Albert Banchs, Ignacio Soto and Albert Vidal, IEEE 802.21 (Media Independent Handover services) Overview,

[5] Colin R. Miller, Major, USAF Electromagnetic Pulse Threats in 2010, 325 Chennault Circle Maxwell AFB Alabama 36112-6427, November 2005,

[6] D-Link, User Manual DIR-300,

[7] Bickes; A. Ganghofer E., Instrukcja obsługi i konserwacji dla DS110.KS2.F.MP1.B High-Power RF Source HPM DS110.KS2.F.x, Diehl, 20.12.2007r.

Autorzy

mgr inż. Andrzej KACZMAREK, Ośrodek Badawczo-Rozwojowy Centrum Techniki Morskiej, ul. Dickmana 62, 81-109 Gdynia, E-mail: Andrzej.Kaczmarek@ctm.gdynia.pl;

dr inż. Rafał NAMIOTKO, Ośrodek Badawczo-Rozwojowy Centrum Techniki Morskiej, ul. Dickmana 62, 81-109 Gdynia, E-mail: Rafal.Namiotko@ctm.gdynia.pl;.