

# Metoda pomiaru wycieków elektromagnetycznych w oparciu o emisję promieniowaną jednostek centralnych PC

**Streszczenie.** W urządzeniach zabezpieczanych obudowami ekranującymi mamy do czynienia z wyciekami elektromagnetycznymi, które są bardzo trudne do zlokalizowania. W artykule przedstawiono stanowisko do pomiaru emisji promieniowanej urządzeń informatycznych. Ponadto w artykule przedstawiono opracowaną metodę pomiaru wycieków elektromagnetycznych w oparciu o emisję promieniowaną jednostek centralnych PC wraz z algorytmem postępowania. Przedstawiono i omówiono wyniki pomiarów identyfikowania miejsc wycieków elektromagnetycznych.

**Abstract.** The devices secured by shielded enclosures we are dealing with electromagnetic leakage which are very difficult to locate. This paper shows a radiated emission measurement stand emitted by information devices. In addition, the paper presents a method for measuring leakages developed based on electromagnetic emissions radiated by CPUs with the algorithm procedure. This paper presents and discusses the results of measurements of electromagnetic leakage and identification them. **Method for measuring leakages based on electromagnetic emissions radiated by CPUs.**

**Słowa kluczowe:** emisja promieniowana, wycieki elektromagnetyczne, kompatybilność elektromagnetyczna, komputer PC.

**Keywords:** radiated emissions, leakage electromagnetic, electromagnetic compatibility, central unit of PC.

doi:10.12915/pe.2014.07.56

## Wstęp

Wszelkiego rodzaju urządzenia o charakterze elektrycznym i elektronicznym zawsze wprowadzają do środowiska zewnętrznego zaburzenia elektromagnetyczne.

Zaburzenia powodowane emisją pożądaną eliminuje się racjonalną gospodarką widmem elektromagnetycznym, stosując odpowiedni przydział częstotliwości lub pasm roboczych. Natomiast zaburzenia wywołane emisją niepożądaną powinny mieć tak określone poziomy, aby nie zakłócały pracy innych obiektów w miejscu ich zainstalowania. Zagadnienie to powinno być przedmiotem analizy już na etapie projektowania urządzeń.

Energia elektromagnetyczna przedostaje się do otaczającego środowiska na skutek: promieniowania elektromagnetycznego w wolnej przestrzeni, przewodzenia przez przewody zasilające, sygnałowe oraz łączące źródło emisji z otaczającym środowiskiem, sprzężenia pojemnościowego i sprzężenia indukcyjnego.

Zaburzenia są emitowane między innymi przez urządzenia informatyczne i telekomunikacyjne. Urządzenia te powinny być tak zaprojektowane i wykonane, aby w normalnym środowisku elektromagnetycznym były odporne na określony poziom zakłóceń i nie wywoływały zaburzeń elektromagnetycznych o wartościach przekraczających odporność na te zaburzenia innego urządzenia występującego w tym środowisku.

W artykule szczególną uwagę zwrócono na emisję promieniowaną niepożądaną, które są produktem ubocznym, wytwarzanym w sposób niezamierzony podczas realizacji podstawowej funkcji urządzenia. Powstają one w obwodach elektrycznych zawierających indukcyjności i pojemności, w których mają miejsce nagłe zmiany prądu lub napięcia względnie fluktuacyjne zmiany gęstości nośników ładunku elektrycznego lub w których występuje dodatnie sprzężenie zwrotne.

W artykule przedstawiono również analizę emisji promieniowanej dla jednostki centralnej PC oraz wyniki identyfikacji miejsc wycieków elektromagnetycznych dla jednostki centralnej komputera PC cechujących się podwyższoną emisją promieniowaną

## Wycieki elektromagnetyczne

Wbrew pozorom, kradzież informacji poprzez podsłuch fal elektromagnetycznych nie jest jedynie domeną powieści szpiegowskich. Do niedawna odpowiedni sprzęt był kosztowny i w zasadzie był niedostępny poza służbami specjalnymi. Dzisiaj można go kupić za cenę kilkunastu

tysięcy złotych. Niektóre z rozwiązań są tanie, amatorskie wykonanie odbiornika nie przekracza 1000 zł, za jego pomocą można odebrać sygnał typowego laptopa z odległości kilkunastu metrów.

Dane przetwarzane w urządzeniu informatycznym mogą zostać skutecznie zaszyfrowane przed wysyłaniem ich przez sieć lub przy składowaniu na dysku, ale w pamięci operacyjnej komputera albo też na jego monitorze są w postaci czytelnej dla wszystkich. Odebranie fal radiowych powstających przy wyświetlaniu lub przetwarzaniu informacji, daje możliwość ominięcia stosowanego szyfrowania. Starsze komputery posiadały solidną, precyzyjnie spasowaną, stalową obudowę, której elementy łączono przy wykorzystywaniu siatki przewodzącej, wszystkie złącza były dobrze połączone z uwzględnieniem szczelności ekranu i odseparowania prądów przepływających po wewnętrznej jego płaszczyźnie.

Obecne komputery nie mają w ogóle ekranującej obudowy i to jest ich bardzo poważna wada. Ich płyty główne przesyłają bowiem sygnały o częstotliwościach rzędu kilku GHz, stając się nadajnikami radiowymi. Tymczasem sygnały cyfrowe mają bardzo ostre zbocza obwiedni, dzięki czemu posiadają silne wysokie harmoniczne. Dla tych zakresów częstotliwości, dłuższe ścieżki na płytach głównych działają jak antena. Daje się też zauważyć lekceważący stosunek producentów do ekranowania samej płyty. Silne sygnały cyfrowe przesyłane są również z kontrolera twardego dysku do samego urządzenia poprzez kable, które są dobrą anteną nadawczą. Dzisiejsze komputery emitują silne zaburzenia, wynika to stąd, że stosowany w obudowie, tani plastik nie spełnia roli ekranu elektromagnetycznego. Z tego względu pojęcie wycieków elektromagnetycznych z urządzenia informatycznego (jednostki centralnej PC) nabiera dużego znaczenia. W artykule pokazano w jaki sposób można taki wyciek elektromagnetyczny w prosty sposób zlokalizować. Często takim miejscem jest interfejs sprzętowy używany w komputerach PC, przez który fala elektromagnetyczna najczęściej wydostaje się na zewnątrz obudowy.

## Analiza wybranych interfejsów urządzeń informatycznych

Pojęcie „interfejs” definiowane jest jako granica współdzielona przez dwa systemy, programy, urządzenia jak również elementy tej granicy a także pomocnicze układy sterujące, które są wykorzystywane do łączenia urządzeń.

W celu przesyłania danych, muszą one być reprezentowane przez sygnał – proces fizyczny, np. elektromagnetyczny, elektryczny bądź optyczny. Proces fizyczny, który wykorzystuje się do przesyłania sygnałów w interfejsie to oscylacje elektromagnetyczne różnych częstotliwości. Najpopularniejszymi sygnałami elektrycznymi są oscylacje w stosunkowo niskim zakresie częstotliwości: do kilkudziesięciu bądź kilkuset MHz, które przesyłane są w przewodach elektrycznych.

W artykule przedstawiono tylko te interfejsy, które są obecnie powszechnie stosowane w komputerach służących do przetwarzania informacji niejawnych. Ze względu na możliwości przechwycenia informacji i jej rozkodowanie przedstawione zostały dwa wybrane interfejsy z komunikacją szeregową (USB oraz RS-232).

Magistrala USB początkowo miała służyć jako standardowy interfejs do transmisji po liniach telefonicznych. Jednakże okazało się, że można za jej pośrednictwem dołączać urządzenia peryferyjne do komputera. Ten rodzaj złącza umożliwia podłączenie różnego rodzaju urządzeń, m.in. myszki, klawiatury, drukarki, skanera. Kolejną zaletą jest to, że dotychczasowe rozwiązania komunikacji komputera z urządzeniami z wykorzystaniem złączy szeregowych w porównaniu z USB nie zapewniają dużej przepustowości, ani nie zapewniają takiej różnorodności w możliwości podłączania urządzeń.

Transmisja danych może odbywać się przy wykorzystaniu różnego, zależnego od specyfikacji danego urządzenia, pasma. W celu dostosowania szerokości pasma transmisji do wymagań wykorzystywany jest zintegrowany z płytą specjalizowany kontroler. Pakiety danych o różnych długościach przesyłane są do odpowiednich urządzeń z różnymi szybkościami:

- do 1,5 Mb/s: określana jest jako Low Speed i do przykładowych zastosowań można podać podłączenie klawiatury czy myszy. Dane można przesyłać z częstotliwością do 1,5Mb/s
- do 12 Mb/s: określana jako Full Speed, którą stosuje się w celu podłączenia urządzeń do transmisji danych po liniach telefonicznych oraz urządzeń audio. Był to najszybszy tryb wersji USB 1.0
- do 480 Mb/s: określana jest jako Hi-Speed, jest wersją 2.0 tego interfejsu i stosuje się do urządzeń wideo i pamięci dyskowych
- do 5Gb/s: określana jako Super Speed, jest to wersja 3.0 tego interfejsu.

Każda wersja interfejsu USB zapewnia transmisję strumienia bitów z inną częstotliwością. Największa możliwa częstotliwość przesyłania danych wynosi 5Gb/s dla wersji USB 3.0. Dlatego też wzrostu emisji promieniowanej można spodziewać się w zakresie od 30MHz do 6GHz.

Interfejs RS-232 to standard interfejsu szeregowego w komputerach. Systemy operacyjne nadają łączom szeregowym nazwy COMn, gdzie n- oznacza numer łącza. Dzięki temu interfejsowi możliwa jest obsługa modemów oraz podłączanie urządzeń, np. myszy lub drukarki.

Podczas przesyłania informacji między komputerami a siecią telekomunikacyjną z wykorzystaniem modemów wyróżnia się dwa rodzaje urządzeń DTE i DCE.

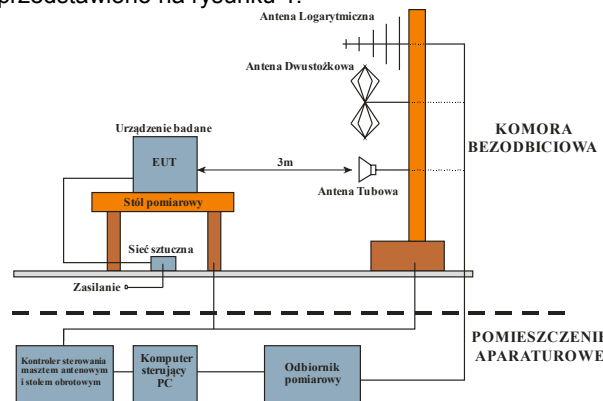
Interfejs RS-232C realizuje transmisję szeregową asynchroniczną. Oznacza to, że komputer wyposażony w to łącze oraz podłączone urządzenie muszą pracować z taką samą, wcześniej uzgodnioną prędkością i jednakową strukturą znaków. Wysyłanie danych może odbywać się w trybie bez potwierdzenia lub z potwierdzeniem odbioru. W tym trybie najmniejszą przesyłaną jednostką jest jeden bajt (jeden znak). Bity przesyła się kolejno. Dla trybu asynchronicznego przyjmuje się zbiór standardowych szybkości transmisji: 50, 75, 110, 150, 300, 600, 1200,

2400, 4800, 9600, 19200, 38400, 57600 oraz 115200 b/s. W trybie synchronicznym interfejs RS-232C pozwala na przesyłanie danych z szybkością do 1Mb/s. Dlatego też wzrostu emisji promieniowanej można spodziewać się w zakresie od 30MHz do 1GHz.

### Stanowisko pomiarowe do pomiaru emisji promieniowanej

Pomiary zaburzeń promieniowanych emitowanych przez urządzenia informatyczne przeprowadzono zgodnie z normą PN-EN 55022:2006. Polegają one na pomiarze natężenia pola elektromagnetycznego w odległości 3m od urządzenia za pomocą anten pomiarowych i odbiornika pomiarowego w zakresie częstotliwości od 30MHz do 6000MHz. Pomiary przeprowadza się dla polaryzacji pionowej i poziomej anten pomiarowych oraz dla poszczególnych kombinacji położenia obiektu badań. Położenie obiektu badań względem anteny pomiarowej jest zmieniane za pomocą stołu obrotowego i maszty antenowego automatycznie. Uzyskane jest to dzięki wykorzystaniu odpowiedniego kontrolera sterującego stołem obrotowym i wysokością maszty antenowego oraz komputera sterującego całym procesem pomiarowym.

Do pomiarów zaburzeń promieniowanych konieczne jest zestawienie stanowiska pomiarowego w konfiguracji jaką przedstawiono na rysunku 1.



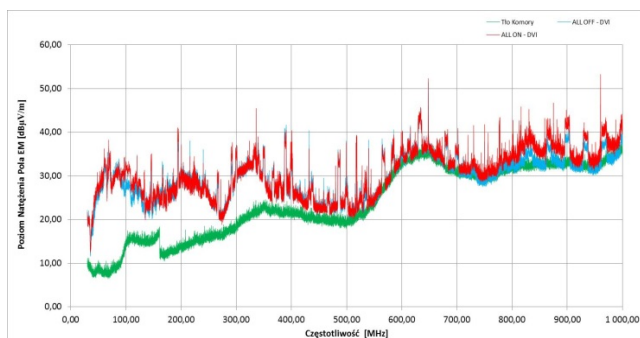
Rys. 1. Schemat blokowy stanowiska pomiarowego do pomiaru emisji promieniowanych

W czasie pomiarów należy zmieniać wysokość położenia anteny w granicach od 1m do 4m w celu znalezienia maksymalnych wskazań przy każdej częstotliwości pomiarowej oraz zmieniać azymut anteny względem badanego urządzenia w celu znalezienia maksymalnych wskazań. Dla ułatwienia pomiarów badane urządzenie może być obracane przy stałym położeniu anteny. Jeśli jest to niemożliwe, to należy wykonywać pomiary, przesuwając antenę wokół badanego, nieruchomego urządzenia. Podczas pomiarów należy zmieniać polaryzację anteny (pozioma lub pionowa) względem badanego urządzenia w celu określenia maksymalnych wskazań.

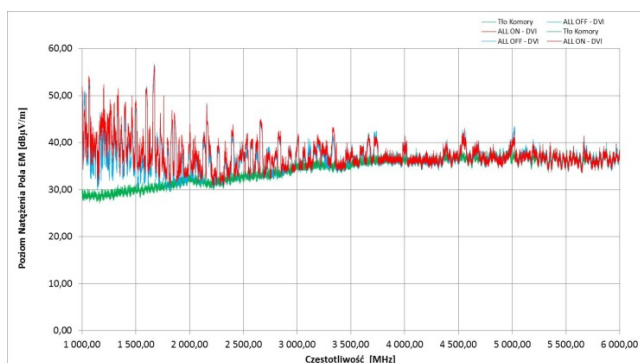
### Wyniki pomiarów oraz analiza emisji promieniowanej dla jednostki centralnej PC

Pomiary poziomów zaburzeń emisji promieniowanej emitowanej przez urządzenia informatyczne przeprowadzono na określonej ilości sztuk urządzeń w odległości 3m od badanego urządzenia. Na podstawie uzyskanych wyników pomiarowych uśredniono wyniki pomiarów oraz dokonano analizy poziomów emisyjności promieniowanej współczesnych urządzeń informatycznych. Pomiary dokonano w zakresie częstotliwości od 30MHz do 6000MHz wykorzystując detektor wartości szczytowej, bazując na metodyce zgodnej z normą PN-EN 55022.

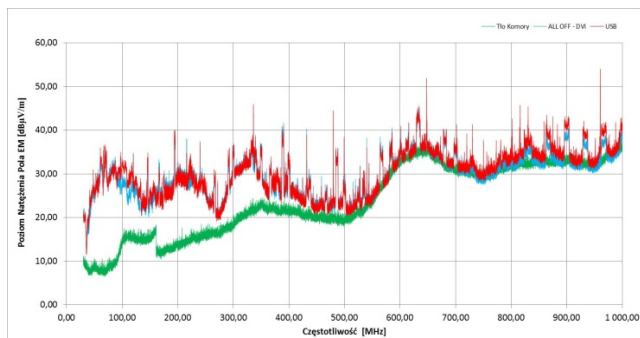
Na rysunkach 2 i 3 pokazano uśrednione z 5 pomiarów poziomy pomierzonych wartości natężenia pola elektromagnetycznego promieniowanego przez jednostkę centralną PC przy pracy wszystkich komponentów.



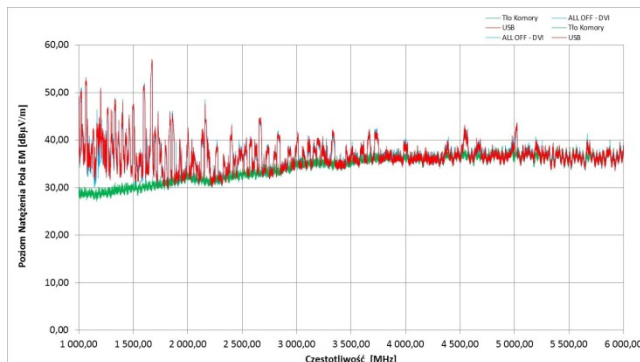
Rys. 2. Uśrednione z 5 pomiarów poziomy emisji promieniowanej emitowanej przez jednostkę centralną PC przy pracy wszystkich komponentów w zakresie od 30 MHz do 1000MHz



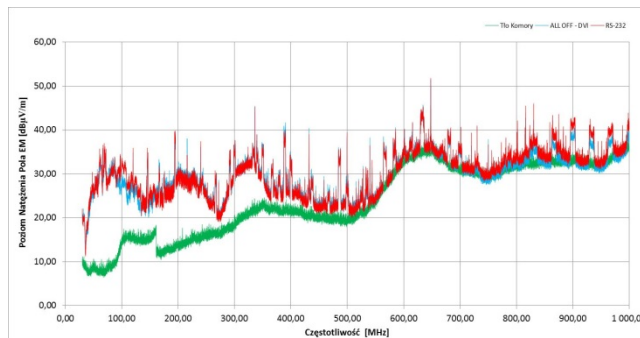
Rys. 3. Uśrednione z 5 pomiarów poziomy emisji promieniowanej emitowanej przez jednostkę centralną PC przy pracy wszystkich komponentów w zakresie od 1 GHz do 6 GHz



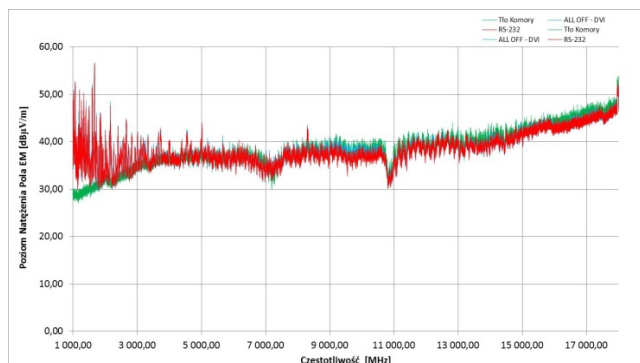
Rys. 4. Uśrednione z 5 pomiarów poziomy emisji promieniowanej emitowanej przez jednostkę centralną PC przy pracy interfejsu USB w zakresie od 30 MHz do 1000MHz



Rys. 5. Uśrednione z 5 pomiarów poziomy emisji promieniowanej emitowanej przez jednostkę centralną PC przy pracy interfejsu USB w zakresie od 1 GHz do 6 GHz



Rys. 6. Uśrednione z 5 pomiarów poziomy emisji promieniowanej emitowanej przez jednostkę centralną PC przy pracy interfejsu RS232 w zakresie od 30 MHz do 1000MHz



Rys. 6. Uśrednione z 5 pomiarów poziomy emisji promieniowanej emitowanej przez jednostkę centralną PC przy pracy interfejsu RS232 w zakresie od 1 GHz do 6GHz

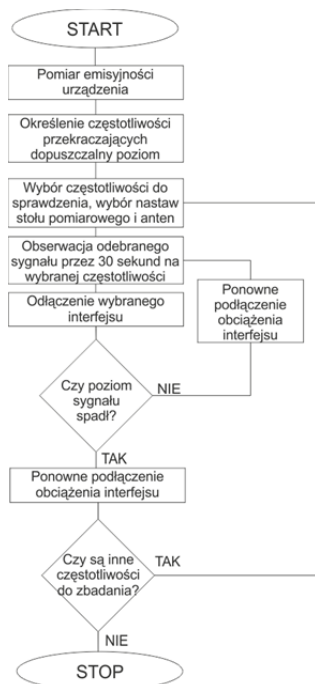
Na rysunkach 4 i 5 pokazano uśrednione z 5 pomiarów poziomy pomierzonych wartości natężenia pola elektromagnetycznego promieniowanego przez jednostkę centralną PC przy pracy wyłącznie interfejsu USB.

Na rysunkach 6 i 7 pokazano uśrednione z 5 pomiarów poziomy pomierzonych wartości natężenia pola elektromagnetycznego promieniowanego przez jednostkę centralną PC przy pracy wyłącznie interfejsu RS-232.

Na wszystkich przedstawionych powyżej rysunkach kolorem zielonym pokazano poziomy tła szumowego występującego w komorze bezodbiwojowej, kolorem niebieskim pokazano uśrednione poziomy emisji promieniowanej pochodzące od jednostki centralnej PC w stanie pracy czuwania (włączony system operacyjny), natomiast kolorem czerwonym pokazano uśrednione poziomy emisji promieniowanej pochodzące od jednostki centralnej PC w stanie pracy poszczególnych interfejsów (np. USB lub RS-232).

Na bazie wyników pomiarowych można określić miejsca wycieków elektromagnetycznych z obudowy jednostki centralnej PC, poprzez interfejsy zewnętrzne tej jednostki. Cały proces zlokalizowania wycieków elektromagnetycznych poprzez zewnętrzne interfejsy sprzętowe jednostki centralnej PC odbywa się według algorytmu przedstawionego na rysunku 7.

Pierwszym etapem jest określenie częstotliwości, na których widoczne były zwiększone wartości emisyjności. Jest to możliwe poprzez odczytanie bezpośrednio z wyników pomiarowych wartości częstotliwości. Na tej podstawie wybrane zostały częstotliwości na których dokonano analizy emisji promieniowanej. Następnie dla wszystkich wybranych częstotliwości dokonywano obserwacji poziomu sygnału przez 30 sekund przy zachowaniu nastaw stołu i anten pomiarowych jak podczas wykonywania wcześniejszych pomiarów.



Rys. 7. Algorytm określający metodę wyszukiwania interfejsu sprzętowego o zwiększonej emisji

Następnie metodą eliminacji odłączane są kolejne obciążenia interfejsów sprzętowych komputera PC celem ponownej obserwacji emisji na danej częstotliwości. Jeśli emisja spadła oznacza to, że został w ten sposób zidentyfikowany interfejs sprzętowy powodujący zwiększenie wartości emisyjności. Dzięki temu zlokalizowane zostało miejsce wycieku elektromagnetycznego. W przeciwnym wypadku należy kontynuować odłączanie komponentów. Następnie interfejs był ponownie obciążany poprzez podłączenie pętli do komputera PC, ponieważ nie można wykluczyć, że powoduje on podbicia emisyjności na nie więcej niż jednej częstotliwości. Powyższa czynność służy do identyfikacji wycieku elektromagnetycznego dla pojedynczej częstotliwości. W tym momencie należy przystąpić do sprawdzenia czy wszystkie z przygotowanych wcześniej częstotliwości zostały przebadane. Jeśli nie to należy przejść do badania następnej z wyselekcjonowanych częstotliwości. Procedura zostaje ukończona w momencie gdy zostaną zlokalizowane wszystkie miejsca, z których emitowana jest podwyższona emisja, a tym samym wszystkie miejsca wycieków elektromagnetycznych.

## Wnioski

Wszystkie urządzenia elektroniczne zasilane energią elektryczną, czy to w obudowie, czy bez obudowy wytwarzają pole elektromagnetyczne, które może być zarejestrowane i w późniejszym czasie zdekodowane. Praktyczną ochronę przed wyciekami elektromagnetycznymi uzyskuje się poprzez zastosowanie ekranowania elektromagnetycznego (ekranowanie) oraz stosowanie filtrów na przewodach zasilania i sygnałowych. Niestety coraz częściej obecne komputery nie mają w ogóle ekranującej obudowy i to jest ich bardzo poważna wada. Ich płyty główne przesyłają bowiem sygnały o częstotliwościach rzędu kilku GHz, stając się źródłami fal elektromagnetycznych. W urządzeniach niezabezpieczonych czy zabezpieczonych obudowami ekranującymi mamy zawsze do czynienia z wyciekami elektromagnetycznymi, które są bardzo trudne do zlokalizowania.

W artykule przedstawiono i omówiono wyniki pomiarów identyfikowania miejsc wycieków elektromagnetycznych bazując bezpośrednio na emisji promieniowanej badanego urządzenia elektronicznego przy pomocy emisyjności urządzenia przy wyłączonym interfejsie oraz emisyjności urządzenia przy włączonym interfejsie. Porównując te dwa widma emisyjności urządzenia jesteśmy w stanie określić miejsca wycieków elektromagnetycznych i częstotliwości przy których taki wyciek ma miejsce. Jednak dokładniejszą metodą określenia miejsca wycieku elektromagnetycznego z jednostki centralnej PC jest opracowana i omówiona metoda pomiaru wycieków elektromagnetycznych w oparciu o emisję promieniowaną jednostek centralnych PC wraz z algorytmem postępowania.

W artykule również określono i oszacowano uśrednione poziomy promieniowanych emisji niepożądanych pochodzących od współczesnego sprzętu informatycznego (wybrana jednostka centralna PC). Emisje te są produktem ubocznym, wytwarzanym w sposób niezamierzony podczas realizacji podstawowej funkcji urządzenia, a zatem należy dążyć do tego aby ich poziom był jak najmniejszy.

Ponadto dzięki identyfikacji miejsc wycieków elektromagnetycznych komponentów wewnętrznych komputera PC powodujących podwyższoną emisję istnieje możliwość znacznego przyspieszenia procesu przygotowania urządzenia do sprzedaży w przypadku gdy jego poziom emisyjności jest niezgodny z normą.

*Projekt jest finansowany ze środków NCBiR w ramach Umowy NR 0024/R/ID2/2012/02 w latach 2012 – 2015.*

## LITERATURA

- [1] PN-EN 55022:2006: *Kompatybilność elektromagnetyczna (EMC) - Urządzenia informatyczne - Charakterystyki zaburzeń radioelektronicznych - Poziomy dopuszczalne i metody pomiaru*; Polski Komitet Normalizacyjny, (2006)
- [2] Gook M. „*Interfejsy sprzętowe komputerów PC*”, Helion, Gliwice (2005).
- [3] Rotkiewicz W. „*Kompatybilność elektromagnetyczna w radiotechnice*”, WKiŁ, Warszawa (1978).
- [4] Przesmycki R., Wnuk M., Nowosielski L., Piwowarczyk K, Bugaj M. „*The Conducted and Radiated Emission Levels from IT Devices*”, PIERS Proceedings (2012), str. 77-81, ISSN 1559-9450, ISBN: 978-1-934142-20-2.
- [5] Przesmycki R., Wnuk M., Nowosielski L., Piwowarczyk K, Bugaj M. „*Analysis of the Radiated Emissions of IT Equipment*”, PIERS Proceedings (2012), str. 1419-1423, ISSN 1559-9450, ISBN: 978-1-934142-22-6,
- [6] Przesmycki R., Wnuk M., Nowosielski L., Bugaj M. „*Analysis of conducted and radiated emission from IT devices in the frequency band 0,15MHz – 6000MHz*”, IEEE Xplore, ISSN: 2157-9822, Print ISBN: 978-1-4577-1814-4

**Autorzy:** mgr inż. Rafał Przesmycki, Wojskowa Akademia Techniczna, Wydział Elektroniki, ul. Gen S. Kaliskiego 2, 00-908 Warszawa, E-mail: [rprzesmycki@wat.edu.pl](mailto:rprzesmycki@wat.edu.pl); prof. dr hab. inż. Marian Wnuk, Wojskowa Akademia Techniczna, Wydział Elektroniki, ul. Gen S. Kaliskiego 2, 00-908 Warszawa, E-mail: [mwnuk@wat.edu.pl](mailto:mwnuk@wat.edu.pl)