

# AUTOREFERAT

## SPIS TREŚCI

<b>1.</b>	<b>IMIĘ I NAZWISKO.....</b>	<b>3</b>
<b>2.</b>	<b>POSIADANE DYPLOMY, STOPNIE NAUKOWE – Z PODANIEM NAZWY, MIEJSCA I ROKU ICH UZYSKANIA ORAZ TYTUŁU ROZPRAWY DOKTORSKIEJ .....</b>	<b>3</b>
<b>3.</b>	<b>INFORMACJE O DOTYCHCZASOWYM ZATRUDNIENIU W JEDNOSTKACH NAUKOWYCH.....</b>	<b>3</b>
<b>4.</b>	<b>WSKAZANIE OSIĄGNIĘCIA WYNIKAJĄCEGO Z ART. 16 UST. 2 USTAWY Z DNIA 14 MARCA 2003 R. O STOPNIACH NAUKOWYCH I TYTULE NAUKOWYM ORAZ O STOPNIACH I TYTULE W ZAKRESIE SZTUKI (DZ. U. 2016 R. POZ. 882 ZE ZM. W DZ. U. Z 2016 R. POZ. 1311.) .....</b>	<b>4</b>
4.1.	TYTUŁ OSIĄGNIĘCIA .....	4
4.2.	OMÓWIENIE CELU NAUKOWEGO PRACY I OSIĄGNIĘTYCH WYNIKÓW WRAZ Z OMÓWIENIEM ICH EWENTUALNEGO WYKORZYSTANIA.....	4
<b>5.</b>	<b>OMÓWIENIE POZOSTAŁYCH OSIĄGNIĘĆ NAUKOWO-BADAWCZYCH .....</b>	<b>12</b>
<b>6.</b>	<b>LITERATURA .....</b>	<b>19</b>

## 1. Imię i nazwisko

Leszek, Józef Nowosielski

## 2. Posiadane dyplomy, stopnie naukowe – z podaniem nazwy, miejsca i roku ich uzyskania oraz tytułu rozprawy doktorskiej

- 1) Dyplom uzyskania tytułu zawodowego: *magister inżynier elektronik*  
specjalność: *eksploatacja systemów łączności*  
miejsce i rok uzyskania: *Wydział Elektroniki, Wojskowa Akademia Techniczna, 1990 r.*
- 2) Dyplom uzyskania stopnia naukowego: *doktor nauk technicznych (Załącznik nr 1)*  
dyscyplina: *telekomunikacja*  
specjalność: *radiokomunikacja*  
miejsce i rok uzyskania: *Wydział Elektroniki, Wojskowa Akademia Techniczna, 1998*  
tytuł rozprawy doktorskiej: *Efektywność kodów splotowych w kanałach zakresu krótkofalowego*
- 3) Świadcstwo: *znajomości języka angielskiego nr 4171/03, poziom III<sup>0</sup> zgodnie ze STANAG 6001 (Załącznik nr 6, str. 16)*  
miejsce i rok uzyskania: *Centralna Komisja Egzaminacyjna Języków Obcych Ministerstwa Obrony Narodowej, Warszawa, 2003*
- 4) Świadcstwo: *znajomości języka rosyjskiego nr 774, poziom I<sup>0</sup> zgodnie ze STANAG 6001 (Załącznik nr 6, str. 17)*  
miejsce i rok uzyskania: *Wojskowa Akademia Techniczna, 2002*
- 5) Certyfikowany Kierownik Projektu: *Certyfikat PRINCE2 Foundation. Certyfikat nr 15765/2013 (APM Group Ltd.) (Załącznik nr 6, str. 18)*
- 6) Certyfikowany Kierownik Projektu: *Certyfikat PRINCE2 Practitioner. Certyfikat nr 18951/2014 (EXIN) (Załącznik nr 6, str. 19)*

## 3. Informacje o dotychczasowym zatrudnieniu w jednostkach naukowych

Lp.	Miejsce zatrudnienia	Okres	Etat	Stanowisko
1.	Brygada Łączności w Wałczu	1990-1991		Dowódca plutonu radiowego
2.	Instytut Systemów Łączności, Wydział Elektroniki, Wojskowa Akademia Techniczna	1991-1993	inżynier	-
3.	Instytutu Telekomunikacji, Wydział Elektroniki, Wojskowa Akademia Techniczna	1993-2005	asystent	-
4.		2005-2007	adiunkt	Z-ca Kierownik Laboratorium Kompatybilności Elektromagnetycznej ds. Technicznych
5.		2007-aktualnie	adiunkt	Kierownik Laboratorium Kompatybilności Elektromagnetycznej

#### **4. Wskazanie osiągnięcia wynikającego z art. 16 ust. 2 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz. U. 2016 r. poz. 882 ze zm. w Dz. U. z 2016 r. poz. 1311.)**

##### **4.1. Tytuł osiągnięcia**

**L. Nowosielski**, *Minimalizacja elektromagnetycznej podatności infiltracyjnej urządzeń informatycznych*, Monografia habilitacyjna, Wojskowa Akademia Techniczna, Warszawa, 2019 r., ilość stron 212, ISBN: 978-83-7938-198-2 (**Załącznik nr 4**).

Recenzenci wydawniczy:

- **dr hab. inż. Piotr Kaniewski, prof. WAT**, Instytut Radioelektroniki, Wydział Elektroniki, Wojskowa Akademia Techniczna.
- **dr hab. inż. Piotr Słobodzian, prof. PWr**, Katedra Telekomunikacji i Teleinformatyki, Wydział Elektroniki, Politechnika Wrocławska.

##### **4.2. Omówienie celu naukowego pracy i osiągniętych wyników wraz z omówieniem ich ewentualnego wykorzystania**

W trakcie realizacji prac badawczych w 2019 r. nakładem Wydawnictwa Wojskowej Akademii Technicznej, wydałem monografię habilitacyjną pod tytułem *Minimalizacja elektromagnetycznej podatności infiltracyjnej urządzeń informatycznych*, złożoną z pięciu rozdziałów podsumowanych zakończeniem oraz czterech dodatków. Recenzentami wydawniczymi mojej monografii byli dr hab. inż. Piotr Słobodzian (Politechnika Wrocławska) oraz dr hab. inż. Piotr Kaniewski (Wojskowa Akademia Techniczna). W dalszej części niniejszego opracowania przedstawiłem cel naukowy pracy oraz osiągnięte wyniki z uwypukleniem mojego autorskiego wkładu na tle aktualnego stanu wiedzy w obszarze obejmującym tematykę monografii. W opracowaniu omówiono także zastosowanie osiągniętych wyników.

Każde urządzenie elektroniczne jest źródłem niepożądanych zaburzeń generowanych jako emisja zaburzeń promieniowanych [4] [6] [35] [38] [40] oraz przewodzonych [6] [29] [36] [37], które są potencjalnymi emisjami ujawniającymi promieniowanymi oraz przewodzonymi. W sprzyjających warunkach możliwe jest wykorzystanie niepożądanego emisji zaburzeń w procesie infiltracji elektromagnetycznej. Zagadnienia dotyczące technicznych metod przeprowadzania infiltracji elektromagnetycznej urządzeń informatycznych oraz zagrożeń z tym związanych są poruszane w nielicznych polskojęzycznych pozycjach literaturowych [20] [21] [42] oraz anglojęzycznych artykułach [17] [18] [24] [28] [63] [64] [65]. Zdaniem autora, najpełniejsze jak dotąd monograficzne przedstawienie zagadnień związanych z zagadnieniami infiltracji elektromagnetycznej urządzeń informatycznych zaprezentowano w pracy [28].

Monografia dotyczy zagrożeń związanych z nieuprawnionym pozyskiwaniem informacji przetwarzanej w urządzeniach informatycznych na podstawie emisji ujawniających promieniowanych i przewodzonych oraz sposobów zabezpieczania tych urządzeń przed infiltracją elektromagnetyczną.

**Zasadniczym celem naukowym monografii jest:**

- **analiza aktualnego stanu wiedzy w zakresie metod pomiaru poziomu emisji zaburzeń elektromagnetycznych generowanych przez urządzenia informatyczne,**
- **opracowanie nowych metod oceny jakości wyników pomiaru poziomu emisji zaburzeń elektromagnetycznych,**

- **zaprezentowanie metody identyfikacji emisji ujawniających generowanych nieintencjonalnie przez urządzenia informatyczne,**
- **określenie wymagań na wartości parametrów zabezpieczeń urządzeń informatycznych, które minimalizują ryzyko elektromagnetycznego przenikania informacji oraz ocena ich skuteczności metodą badań laboratoryjnych oraz symulacji komputerowych.**

W Rozdziale 1 monografii przedstawiłem aktualny stan wiedzy w obszarze obejmującym tematykę monografii oraz na tym tle opisałem swój indywidualny dorobek badawczy opisany szczegółowo w dalszych rozdziałach opracowania.

*W celu wykazania istnienia poważnego zagrożenia infiltracją elektromagnetyczną w stosunku do współczesnych urządzeń informatycznych w Rozdziale 2.1 opisałem metodę testu podatności infiltracyjnej jednego z szerokopasmowych interfejsów urządzeń informatycznych wykorzystujących szeregową transmisję danych jakim jest interfejs USB 2.0. Przedstawiona w monografii metodyka bazuje na wykorzystaniu podczas badań programowego generatora wymuszeń sygnałów GWS, którego zadaniem jest generowanie sygnału testowego na wyjściu badanego interfejsu urządzenia informatycznego. Zbliżony do proponowanego w monografii algorytm postępowania wykorzystujący GWS w celu identyfikacji emisji ujawniających generowanych przez wąskopasmowe interfejsy takie jak: RS-232, PS/2 i VGA został opisany w polskojęzycznych [20] [21] oraz anglojęzycznych pozycjach literaturowych [24] [28] [63] [64] [65]. W monografii zaproponowano opracowane przez autora rozwinięcie opisywanych w istniejących pozycjach literaturowych metodyk wykorzystujących GWS polegające na opracowaniu dedykowanych dla interfejsu USB 2.0:*

- *testowych ciągów informacyjnych generowanych przez GWS,*
- *schematu blokowego stanowiska laboratoryjnego,*
- *testowych częstotliwości dystynktywnych dla emisji ujawniających,*
- *metod obróbki sygnału emisji ujawniającej,*
- *miar stopnia skorelowania sygnału emisji ujawniającej z testowymi ciągami informacyjnymi generowanymi przez GWS.*

*Przedstawioną w monografii metodykę po pewnych modyfikacjach można wykorzystać do przeprowadzenia testów podatności infiltracyjnej innych współczesnych szerokopasmowych interfejsów urządzeń informatycznych, które przetwarzają dane w sposób szeregowy takich jak: USB 1.0, USB 3.0, SATA, LAN i HDMI.*

W celu minimalizacji elektromagnetycznej podatności infiltracyjnej urządzeń informatycznych najczęściej stosuje się zabezpieczenia takie jak obudowy ekranujące lub filtry linii zasilania, których zadaniem jest stłumienie poziomu emisji zaburzeń. W celu oszacowania wymaganego tłumienia poziomu niepożądanych emisji zaburzeń wnoszonego przez stosowane zabezpieczenia, do poziomu utrudniającego odtworzenie informacji przez nie przenoszonych, niezbędna jest znajomość maksymalnych poziomów emisji zaburzeń generowanych przez urządzenia informatyczne.

*W Rozdziale 2.2 przedstawiłem w sposób kompleksowy metodyki pomiaru poziomu emisji zaburzeń promieniowanych i przewodzonych oraz metody szacowania niepewności pomiaru. Zaproponowane budżety szacowania niepewności pomiaru w dalszej części monografii (dodatek B) wykorzystalem do wyznaczenia zależności analitycznych służących do oceny niepewności pomiarów pośrednich takich parametrów jak: skuteczność ekranowania obudowy ekranującej, tłumienność wnoszona przez filtry sieciowe oraz straty absorpcyjne materiałów. Opisane metodyki pomiaru poziomu emisji zaburzeń zostały zaimplementowane przez zespół, którego jestem członkiem w Laboratorium Kompatybilności Elektromagnetycznej Wydziału Elektroniki WAT i uzyskały akredytację Polskiego Centrum Akredytacji (numer akredytacji AB 639).*

W żadnej znanej mi publikacji w obszarze kompatybilności elektromagnetycznej EMC (ang. ElectroMagnetic Compatibility) dotyczącej metodyk pomiaru poziomu za-

burzeń promieniowanych oraz przewodzonych [12] [13] [14] [19] [29] [46] [55] , poza pozycją [59] , nie przedstawiono w sposób kompleksowy opisu metodyki pomiaru poziomu emisji zaburzeń oraz odpowiadających im budżetów szacowania niepewności pomiaru w jednej pozycji literaturowej. Zagadnienia dotyczące metod szacowania niepewności pomiaru są obszernie omawiane m.in. w pozycjach literaturowych [2] [11] [52] [58] [59] , spośród których jedynie książka [59] oraz opracowania [52] [58] dotyczą szacowania niepewności pomiaru poziomu emisji zaburzeń w obszarze kompatybilności elektromagnetycznej EMC (ang. ElectroMagnetic Compatibility). Zdaniem autora monografii w literaturze dotyczącej obszaru EMC nie występuje pozycja literaturowa podająca w sposób bezpośredni zależności analityczne służące do oceny niepewności pomiaru skuteczności ekranowania obudów ekranujących, tłumienności wnoszonej przez filtry sieciowe oraz strat absorpcyjnych materiałów.

Jednym z istotnych narzędzi służących zapewnieniu jakości wyników pomiarów poziomu emisji zaburzeń promieniowanych i przewodzonych zalecanych przez dokument standaryzacyjny [49] jest udział laboratoriów badawczych wykonujących tego typu pomiary w porównaniach międzylaboratoryjnych i wykorzystywanie uzyskiwanych w nich wyników podczas podejmowania odpowiednich działań np. korygujących w stosunku do opracowanych przez laboratoria budżetów niepewności pomiaru poziomu emisji zaburzeń elektromagnetycznych. Zgodnie z wymaganiami Polskiego Centrum Akredytacji [8] w celu określenia zdolności laboratorium akredytowanego do realizacji określonego badania niezbędne jest okresowe przeprowadzanie porównań międzylaboratoryjnych z innymi laboratoriami wykonującymi takie same lub podobne badania. Techniki statystyczne zalecane przez istniejące pozycje literaturowe [23] [50] są bardzo skromnie opisywane i bardzo często nie są dopasowane do potrzeb wynikających ze specyfiki pomiaru poziomu emisji zaburzeń elektromagnetycznych. Z tego też powodu w monografii opisano znaczne rozwinięcie zalecanych technik statystycznej obróbki wyników pomiarowych. *Opisane w Rozdziale 2.3 monografii metody i kryteria oceny jakości wyników pomiarów poziomu emisji zaburzeń uzyskane przez laboratoria badawcze metodą porównań międzylaboratoryjnych nie były wcześniej publikowane w żadnej znanej mi publikacji poza publikacjami [34] [45] , których jestem współautorem. Przedstawione w monografii metody i kryteria oceny jakości wyników pomiarów poziomu emisji zaburzeń wykorzystano podczas porównań międzylaboratoryjnych zorganizowanych w 2006 r. Autor monografii był członkiem zespołu, który organizował powyższe przedsięwzięcie oraz analizował otrzymane wyniki. Raport z przeprowadzonych porównań międzylaboratoryjnych został opublikowany jako pozycja literaturowa [34] .*

Istnienie zagrożeń polegających na możliwości wykorzystania emisji zaburzeń nieintencjonalnie generowanych przez urządzenia informatyczne do odtworzenia przez nieupoważnione osoby przetwarzanej w urządzeniu informacji stwarza konieczność ich przeciwdziałaniu. W praktyce jako zabezpieczenia konstrukcyjne urządzeń informatycznych najczęściej stosowane są zabezpieczenia w formie obudów ekranujących cechujących się odpowiednią dodatkową wartością skuteczności ekranowania oraz zabezpieczenia w formie filtrów linii zasilania sieci energetycznej niskiego napięcia zabezpieczających przed elektromagnetycznym przenikaniem informacji cechujących się odpowiednią dodatkową wartością tłumienia. W celu zabezpieczenia urządzeń informatycznych niezbędnym jest określenie wymaganego dodatkowego tłumienia stosowanych zabezpieczeń.

*W Rozdziale 3 przedstawiłem analizę mającą na celu identyfikację oraz oszacowanie wartości parametrów mających wpływ na wymagane dodatkowe tłumienie stosowanych zabezpieczeń urządzeń informatycznych do poziomu umożliwiającego ich bezpieczne wykorzystanie przy przetwarzaniu informacji. W przeprowadzonej analizie wykorzystalem dane wejściowe dostępne w literaturze technicznej oraz dane otrzymane w wyniku samodzielnych badań przeprowadzonych na potrzeby monografii (np. wyniki pomiarów poziomu szumów środowiskowych przewodzonych w liniach zasilania sieci energetycznej niskiego*

*napięcia). Przedstawiona autorska analiza jest bardzo szczegółowa i uwzględnia praktycznie wszystkie aspekty związane z: emisją, propagacją, odbiorem i przetwarzaniem emisji zaburzeń elektromagnetycznych generowanych nieintencjonalnie przez urządzenia informatyczne. Oszacowane wartości parametrów mających wpływ na wymagane dodatkowe tłumienie stosowanych zabezpieczeń wykorzystałem w procesie określania wymagań względem dodatkowej skuteczności ekranowania i dodatkowego tłumienia odpowiednio dla obudów ekranujących i filtrów linii zasilania, które minimalizują ryzyko elektromagnetycznego przenikania informacji. Wymagania na poziom tłumienia powyższych zabezpieczeń oszacowałem dla najbardziej prawdopodobnych scenariuszy lokalizacji urządzenia informatycznego względem systemu infiltracyjnego cechujących się najmniejszym tłumieniem wnoszonym przez drogę propagacji emisji ujawniającej i jednocześnie uwzględniających taką lokalizację systemu infiltracyjnego, która zapewnia jego maskowanie. W dostępnej literaturze dotyczącej metod zabezpieczenia urządzeń informatycznych nie spotkałem się dotychczas z żadną publikacją opisującą krok po kroku metodykę wyliczania wymaganego dodatkowego tłumienia stosowanych zabezpieczeń urządzeń informatycznych prowadzącą w konsekwencji do określenia zalecanych wartości zabezpieczeń urządzeń informatycznych. Przedstawione w monografii analizy, zależności analityczne określające wymagane dodatkowe tłumienie stosowanych zabezpieczeń, oszacowane wartości parametrów mających wpływ na wymagane tłumienie oraz w konsekwencji wartości wymaganego dodatkowego tłumienia zabezpieczeń stanowią rezultat moich samodzielnych prac.*

W zakresie technik pomiarów poziomu emisji zaburzeń oraz dopuszczalnych poziomów emisji zaburzeń promieniowanych i przewodzonych, które mogą zakłócać pracę innych urządzeń dużą pomoc niesie inżynieria kompatybilności elektromagnetycznej. Dostępne źródła literaturowe z zakresu kompatybilności elektromagnetycznej [13] [14] [29] [46] [59] [67] nie określają jednak wymagań dotyczących skuteczności ekranowania i dodatkowego tłumienia odpowiednio dla obudów ekranujących i filtrów linii zasilania. Powyższe źródła literaturowe definiują jedynie dopuszczalne przez normy zharmonizowane z Dyrektywą Parlamentu Europejskiego i Rady 2014/30/UE [10] poziomy emisji zaburzeń generowanych przez urządzenia informatyczne. Ponadto stosowanie zaleceń z zakresu kompatybilności elektromagnetycznej narzuconych przez normy zharmonizowane z powyższą dyrektywą w stosunku do urządzeń informatycznych nie niweluje zagrożenia infiltracją elektromagnetyczną z powodu zbyt dużego dopuszczalnego przez normy zharmonizowane poziomu zaburzeń promieniowanych oraz przewodzonych. W związku z powyższym stosowanie zaleceń norm zharmonizowanych nie niweluje zagrożenia infiltracją elektromagnetyczną w stosunku do współczesnych urządzeń informatycznych, a jedynie może w sposób pośredni wpływać na zmniejszenie poziomu emisji ujawniających.

W porównaniu ze standardowymi przedsięwzięciami z zakresu kompatybilności elektromagnetycznej w badaniach bezpieczeństwa emisji urządzeń informatycznych przetwarzających informacje niejawnie określa się nie tylko dopuszczalne poziomy natężenia pola emisji zaburzeń promieniowanych i napięcia emisji zaburzeń przewodzonych, które są potencjalnymi emisjami ujawniającymi, ale też wymagania dotyczące parametrów zabezpieczeń urządzeń informatycznych, których spełnienie jest konieczne w procesach certyfikacji tych urządzeń przeprowadzanych przez krajową władzę bezpieczeństwa. Tylko takie urządzenia informatyczne, które przeszły proces certyfikacji z wynikiem pozytywnym, mogą być stosowane przez instytucje i agendy rządowe oraz inne jednostki zajmujące się przetwarzaniem informacji niejawnych w rozumieniu Ustawy o ochronie informacji niejawnych [61]. Niestety oficjalna wiedza [31] [32] z powyższego zakresu, dotycząca wymagań co do zabezpieczenia urządzeń informatycznych, nie jest powszechnie udostępniana w literaturze fachowej z uwagi na zagrożenie jej ewentualnego wykorzystania przez nieupoważnione osoby do wrogiej infiltracji elektromagnetycznej.

Przetwarzanie informacji niejawnych w rozumieniu Ustawy o ochronie informacji niejawnych [61] jest dozwolone wyłącznie z wykorzystaniem urządzeń informatycznych certyfikowanych przez krajową władzę bezpieczeństwa. Poważnymi barierami w stosowaniu urządzeń informatycznych certyfikowanych przez krajową władzę bezpieczeństwa są ich wysoka cena oraz konieczność objęcia ich specjalnym nadzorem, co niejednokrotnie wyklucza możliwość ich stosowania przez małe i średnie firmy z powodów ekonomicznych. Stosowanie urządzeń informatycznych certyfikowanych przez krajową władzę bezpieczeństwa nie jest obowiązkowe w przypadku przetwarzania informacji wewnętrznych przedsiębiorstw nie objętych Ustawą o ochronie informacji niejawnych [61]. Rodzaj technicznych środków zapewnienia bezpieczeństwa użytych do przetwarzania informacji wewnętrznych np. przedsiębiorstwa jest uzależniony wyłącznie od decyzji właściciela tychże informacji.

Powyżej opisane zagrożenia oraz ograniczony dostęp do oficjalnych dokumentów [31] [32] opisujących parametry zabezpieczeń urządzeń informatycznych przeznaczonych do przetwarzania informacji niejawnych w rozumieniu Ustawy o ochronie informacji niejawnych [61] stały się inspiracją dla autora do napisania monografii. Monografia jest dedykowana między innymi producentom i laboratoriom badawczym zajmującym się produkcją oraz badaniami zabezpieczeń urządzeń informatycznych przeznaczonych wyłącznie do przetwarzania informacji nie objętych Ustawą o ochronie informacji niejawnych.

*W Rozdziałach 3.1.2 i 3.2.2 zdefiniowałem zalecane wartości dodatkowej skuteczności ekranowania i dodatkowego tłumienia odpowiednio dla obudów ekranujących i filtrów linii zasilania, które minimalizują ryzyko elektromagnetycznego przenikania informacji. Przedstawione zalecane wartości parametrów zabezpieczeń stanowią rezultat moich samodzielnych prac.*

W przypadku, gdy rzeczywiste wartości skuteczności ekranowania obudów ekranujących i tłumienia wnoszonego przez filtry linii zasilania zastosowane w zabezpieczanym urządzeniu informatycznym będą przyjmowały wartości poniżej zalecanych w monografii, wówczas odbije się to negatywnie na poziomie bezpieczeństwa elektromagnetycznego całego urządzenia informatycznego. W przypadku, gdy rzeczywiste wartości skuteczności ekranowania obudów ekranujących i tłumienia wnoszonego przez filtry linii zasilania zastosowane w zabezpieczanym urządzeniu informatycznym będą przyjmowały wartości powyżej zalecanych w monografii, wówczas odbije się to negatywnie na cenie projektowanej obudowy, a nie wpłynie znacząco na zwiększenie poziomu bezpieczeństwa elektromagnetycznego urządzenia informatycznego. W związku z powyższym w procesie projektowania i konstruowania obudów ekranujących niezbędne jest posiadanie narzędzi umożliwiających pomiar skuteczności ekranowania lub tłumienia niepożądanych sygnałów dla poszczególnych komponentów obudów lub filtrów. Narzędzia powyższe mogą być wykorzystane w celu weryfikacji poprawności działania wykorzystanych zabezpieczeń urządzeń informatycznych.

*W Rozdziale 4 opisałem w sposób kompleksowy narzędzia w formie metod pomiaru oraz symulacji komputerowej skuteczności ekranowania obudów ekranujących o gabarytach mniejszych niż  $1,5\text{ m} \times 1,5\text{ m} \times 1,5\text{ m}$ , tłumienności wnoszonej przez filtry sieciowe i sygnałowe oraz strat absorpcyjnych i rozpraszania materiałów, które mogą być wykorzystane w procesie weryfikacji poprawności działania wykorzystanych zabezpieczeń urządzeń informatycznych. Metody opisane w monografii są kompletne, co umożliwia ich szybką implementację sprzętową lub programową.*

W znanych istniejących publikacjach naukowych [1] [56] [57] [66] [69] [70] oraz dokumentach standaryzacyjnych [22] [47] [48] [51] nt. metodyk pomiaru skuteczności ekranowania obudów ekranujących autorzy zwykle ograniczają opis do podania schematów blokowych i równań opisujących modele pomiaru natomiast nie podają szczegółów technicznych dotyczących implementacji stanowisk badawczych oraz procesu pomiarowego. Z



podobną sytuacją mamy do czynienia w przypadku modeli symulacyjnych przeznaczonych do oceny skuteczności ekranowania obudów. Znane autorowi istniejące publikacje naukowe [62] [68] [71] dotyczące modeli symulacyjnych nie podają szczegółów technicznych dotyczących implementacji programowej.

*O ile opisane w Rozdziale 4.1 metodyki pomiaru oraz symulacji komputerowej skuteczności ekranowania obudów ekranujących i ich komponentów oraz metodyki przedstawione w dostępnej literaturze technicznej są zbliżone i dobrze opisane, to istotne szczegóły dotyczące implementacji stanowisk badawczych oraz procesu pomiarowego są w powyższych dokumentach pomijane lub opisane w sposób pobieżny. Do takich zagadnień należą:*

- algorytmy oprogramowania sterującego procesem pomiarowym,
- metody synchronizacji nadajnika i miernika poziomu sygnału probierczego,
- metody zwiększania zakresu dynamiki pomiaru,
- metody skracania czasu trwania procesu pomiarowego,
- obliczanie skuteczności ekranowania metodą symulacji komputerowej.

*Wartością dodaną monografii są autorskie rozwiązania techniczne dotyczące wyżej wymienionych zagadnień. Rozwiązania powyższe przedstawiłem odpowiednio w Rozdziałach: 4.1.2.1, 4.1.2.2, 4.1.2.3, 4.1.4 i 4.1.5 w trakcie opisywania kolejnych konfiguracji stanowisk pomiarowych wykorzystujących różne typy nadajników oraz mierników poziomu sygnału probierczego. W żadnej znanej autorowi publikacji, poza publikacjami [5] [7] [26] [27] [33] [44], których jestem współautorem, nie przedstawiono rozwiązań technicznych w wersjach prezentowanych w monografii.*

*Na szczególną uwagę czytelnika zasługuje opracowana przeze mnie konfiguracja stanowiska pomiarowego wykorzystująca generator impulsów wysokoenergetycznych opisana w Rozdziale 4.1.4, która oferuje bardzo duży zakres dynamiki pomiaru skuteczności ekranowania obudowy w porównaniu z innymi metodami, a jednocześnie cechuje się bardzo krótkim czasem niezbędnym do przeprowadzenia procesu pomiarowego.*

*Z uwagi na to, że skuteczność ekranowania obudowy jest zależna od rodzaju materiału z jakiego wykonano ekran, a w szczególności parametru materiału jakim są straty absorpcyjne i rozpraszania, w Rozdziale 4.3 zamieściłem opis metodyk umożliwiających pomiar powyższego parametru.*

*O ile metodyki pomiaru poziomu strat absorpcyjnych i rozpraszania materiałów opisane w Rozdziale 4.3.1 oraz metodyki przedstawione w dostępnej literaturze technicznej [16] [25] [60] są zbliżone i dobrze opisane, to metodyka opisana w Rozdziale 4.3.2 wykorzystująca generator impulsów wysokoenergetycznych jest nowatorskim rozwiązaniem, które opracowałem samodzielnie.*

*Podobnie jak w przypadku metodyk pomiaru skuteczności ekranowania obudów tak też i w przypadku metodyk pomiaru tłumienności wnoszonej przez filtry sieciowe i sygnałowe dostępna literatura techniczna [3] [9] [15] [30] nie podaje szczegółów dotyczących implementacji stanowisk badawczych. Wartością dodaną metodyki pomiaru tłumienności filtrów opisanej w Rozdziale 4.2 jest rozwiązanie minimalizujące przenikanie sygnału probierczego z wyjścia generatora sygnału probierczego na wejście miernika poziomu sygnału probierczego poza głównym traktem mierzonego obwodu filtru. Zaproponowane rozwiązanie bazuje na zastosowaniu pomocniczej komory pomiarowej, w której podczas pomiarów jest umieszczany badany filtr. Opisane w monografii rozwiązanie jest kompletne, co umożliwia jego szybką implementację sprzętową i programową. Więcej szczegółów dotyczących powyższego rozwiązania przedstawiono wcześniej w opracowaniu własnym [41].*

*W Rozdziale 5 monografii przedstawiłem opisy przykładowych kompleksowych rozwiązań zabezpieczeń przed elektromagnetycznym przenikaniem informacji w formie komory oraz szafy ekranującej wraz z niezbędnymi filtrami przeznaczonych do instalacji pojedynczego oraz kilku urządzeń informatycznych. W Rozdziale 5 opisałem także rozwiązania konstrukcyjne obudów zintegrowanych z zabezpieczanymi urządzeniami informatycznymi typu komputer PC oraz laptop. Przedstawione rozwiązania zabezpieczeń urzą-*

dzeń informatycznych spełniają określone w monografii wymagania na wartości dodatkowej skuteczności ekranowania i dodatkowego tłumienia odpowiednio dla obudów ekranujących i filtrów linii zasilania, które minimalizują ryzyko elektromagnetycznego przenikania informacji.

*Szereg rozwiązań konstrukcyjnych szaf ekranujących oraz obudów zintegrowanych z zabezpieczonym urządzeniem informatycznym powstało w wyniku projektów, których byłem współwykonawcą w ramach konsorcjum, w skład którego wchodziła Wojskowa Akademia Techniczna oraz firma Siltec Sp. z o.o. (Załącznik nr 5, pkt. III.E, poz. 1). Rozwiązania powyższe były wcześniej opisywane w publikacjach [43] [53] [54], których jestem współautorem. W ramach powyższych projektów brałem udział w opracowaniu oraz wdrożeniu do eksploatacji kompleksowych rozwiązań konstrukcyjnych obudów ekranujących oraz przeprowadziłem badania zgodnie z opracowanymi przez siebie metodykami pomiaru parametrów zastosowanych zabezpieczeń.*

Moje doświadczenia zdobyte podczas realizacji prac badawczych oraz praca w laboratorium kompatybilności elektromagnetycznej<sup>1</sup> umożliwiły przedstawienie w monografii szczegółowych informacji dotyczących kompleksowej metodologii projektowania zabezpieczeń urządzeń informatycznych w formie obudów ekranujących oraz filtrów sieciowych. W literaturze krajowej oraz zagranicznej nie istnieje publikacja o charakterze monograficznym prezentująca powyższe informacje w jednej pozycji literaturowej.

*Do moich najważniejszych oryginalnych osiągnięć w obszarze tematyki zaprezentowanej w monografii można zaliczyć:*

- *opracowanie metodyki testów podatności infiltracyjnej szerokopasmowych interfejsów urządzeń informatycznych przetwarzających dane w sposób szeregowy,*
- *opracowanie metodologii szacowania niepewności pomiaru oraz narzędzi służących zapewnieniu jakości wyników pomiarów poziomu emisji zaburzeń niezbędnych w procesie szacowania wymagań na skuteczności ekranowania i tłumienność wnoszoną odpowiednio dla obudów ekranujących i filtrów linii zasilania, które minimalizują ryzyko elektromagnetycznego przenikania informacji,*
- *wdrożenie do eksploatacji w akredytowanym laboratorium badawczym metodyk oraz stanowisk laboratoryjnych przeznaczonych do pomiaru poziomu emisji zaburzeń promieniowanych oraz przewodzonych,*
- *opracowanie wymagań na skuteczność ekranowania i tłumienie odpowiednio dla obudów ekranujących i filtrów linii zasilania, które minimalizują ryzyko elektromagnetycznego przenikania informacji dla najbardziej prawdopodobnych scenariuszy lokalizacji urządzenia informatycznego względem lokalizacji systemu infiltracyjnego,*
- *przedstawienie oryginalnych wyników pomiarów poziomu szumów środowiskowych przewodzonych w liniach zasilania sieci energetycznej niskiego napięcia wykorzystanych w procesie określania wymagań na tłumienie filtrów sieciowych, które minimalizuje poziom potencjalnych przewodzonych emisji ujawniających,*
- *przedstawienie nowatorskich konfiguracji stanowisk pomiarowych, które można wykorzystać do pomiaru: skuteczności ekranowania obudów ekranujących, tłumienności wnoszonej przez filtry sieciowe i sygnałowe oraz strat absorpcyjnych i rozpraszania materiałów,*
- *opracowanie oryginalnych algorytmów oprogramowania sterującego procesem pomiaru skuteczności ekranowania i pomiaru tłumienności filtrów sieciowych,*
- *opracowanie metody synchronizacji nadajnika i miernika poziomu sygnału probierczego wykorzystywanej w procesie pomiaru skuteczności ekranowania obudów ekranujących przy pomocy stanowiska pomiarowego w konfiguracji wykorzystującej przestrajaną selektywny odbiornik pomiarowy oraz generator sygnałowy,*

---

<sup>1</sup> Autor od 2007 r. do chwili wydania monografii kieruje pracą Laboratorium Kompatybilności Elektromagnetycznej na Wydziale Elektroniki Wojskowej Akademii Technicznej.

- *opracowanie metody zwiększania zakresu dynamiki pomiaru skuteczności ekranowania obudów ekranujących,*
- *opracowanie nowatorskiej metody pomiaru skuteczności ekranowania obudów wykorzystującej wysokoenergetyczne impulsy probiercze wytwarzane przez generator Marksa,*
- *opracowanie oraz wdrożenie do eksploatacji kompleksowych rozwiązań konstrukcyjnych zabezpieczeń przed elektromagnetycznym przenikaniem informacji.*

Należy stwierdzić, że przedstawione w monografii zagadnienia i rozwiązania wybranych problemów związanych z minimalizacją podatności infiltracyjnej współczesnych urządzeń informatycznych nie wyczerpują i nie zamykają tematu, ale w mojej opinii wnoszą istotny wkład do rozwoju tej dziedziny nauki i techniki. Opisane w monografii zagadnienia przyczynią się do podniesienia poziomu bezpieczeństwa informacji przetwarzanych przy pomocy współczesnych urządzeń informatycznych.

## 5. Omówienie pozostałych osiągnięć naukowo-badawczych

Pracę naukowo-dydaktyczną rozpocząłem w Wojskowej Akademii Technicznej 1 września 1991 r., obejmując stanowisko inżyniera w Instytucie Systemów Łączności Wydziału Elektroniki. W 1992 r. ukończyłem *Kurs Edukacji Pedagogicznej* i w 1993 r. zostałem przeniesiony na stanowisko asystenta w zespole pracowników naukowo-dydaktycznych w zakładzie *Radiokomunikacji i walki radioelektronicznej*. W trakcie przeszło dwudziestosiedmioletniej pracy dydaktycznej przeprowadziłem w sumie 6 480 godzin zajęć dydaktycznych. Początkowo prowadziłem ćwiczenia laboratoryjne i rachunkowe z przedmiotów: *Urządzenia i systemy radiokomunikacyjne*, *Radiokomunikacja* oraz *Modulacja i detekcja*. Od 1999 r. prowadzę wykłady z przedmiotów *Kodowanie transmisji radiowych* oraz *Radiokomunikacja ruchoma lądowa*. Natomiast od roku 2005 dodatkowo rozpocząłem wykłady w ramach nowoutworzonych przedmiotów związanych z kompatybilnością elektromagnetyczną *Zagadnienia prawne w elektronice i telekomunikacji* oraz *Kompatybilność elektromagnetyczna*. Moje doświadczenia i wiedza zdobyta podczas realizacji rozprawy doktorskiej pod tytułem *Efektywność kodów splotowych w kanałach zakresu krótkofalowego* pozwoliły mi na stworzenie nowego przedmiotu funkcjonującego pod nazwą *Kodowanie transmisji radiowych*.

W pełni autorski przedmiot *Kodowanie transmisji radiowych*, realizowany obecnie w wymiarze 30 godzin (w tym 10 godzin wykładu, 6 godzin ćwiczeń rachunkowych i 14 godzin laboratorium), obejmuje opracowane przeze mnie następujące treści programowe: system transmisji danych: zakłócenia i błędy w kanałach transmisyjnych, twierdzenie Shannona; modele binarnego kanału transmisji danych oraz ich symulacja komputerowa; kody blokowe: struktura kodu blokowego, zdolność detekcyjna i korekcyjna kodu, geometryczna interpretacja kodu, syndrom, zysk kodu; kodery kodów splotowych: struktura kodu splotowego, metody opisu, zdolność korekcyjna, przebijane kody splotowe; dekodery kodów splotowych: dekodowanie kodów splotowych z maksymalną wiarygodnością, algorytm Viterbiego; symulacja komputerowa pracy kanału kodowego z zastosowaniem metod kodowania korekcyjnego; metody dekorelacji błędów: przeplot blokowy, przeplot splotowy, przeplot heliakalny i losowy; turbo kody: zasada działania, struktura kodera i dekodera; zasada działania modulacji kodowanej kratowo TCM; scrambling: powody stosowania, przykładowe implementacje; wybrane radiowe systemy transmisji danych. Przedmiot wsparty jest autorskim oprogramowaniem napisanym w języku wysokiego poziomu C++ w środowisku Builder podbudowującym zajęcia laboratoryjne.

Kierowałem 70 pracami dyplomowymi oraz zrecenzowałem 46 prac dyplomowych. Jestem autorem jednego skryptu (**Załącznik nr 5, pkt. III.I, poz. 4**) oraz szeregu instrukcji laboratoryjnych dotyczącego budowy i eksploatacji urządzeń radiokomunikacyjnych eksploatowanych w Siłach Zbrojnych RP. Za działalność dydaktyczną zostałem wyróżniony tytułem *Zasłużony nauczyciel akademicki* i *Medalem Komisji Edukacji Narodowej* (**Załącznik nr 5, pkt. III.D, poz. 5 i 12**).

Przez wiele lat byłem opiekunem grup szkoleniowych studentów. Od 2016 r. do chwili obecnej jestem członkiem Rady Naukowej Wydziału Elektroniki. Od 2015 r. do chwili obecnej uczestniczę w pracach *Komisji Rady Wydziału ds. Finansów WEL*. Za całokształt działalności zawodowej zostałem wyróżniony ośmioma medalami resortowymi MON (**Załącznik nr 5, pkt. III.D, poz. 1, 2, 3, 4, 6, 7, 8 i 13**).

Moją działalność naukowo-badawczą można podzielić na dwa zasadnicze okresy. W pierwszym okresie trwającym umownie od 1991 r. do 2004 r. zajmowałem się – w zakładzie Radiokomunikacji i Walki Radioelektronicznej Instytutu Telekomunikacji WEL dydaktyką oraz pracami badawczo-rozwojowymi z zakresu rozpoznawania systemów radiokomunikacyjnych, pomiarze tłumienności kanałów radiowych w celu wyznaczenia stref bezpieczeństwa dla sprzętu teleinformatycznego oraz zagadnieniami związa-

nymi z poprawą wierności transmisji danych w kanałach łączności radiowej. Moje prace badawcze w powyższym zakresie rozwijały się zgodnie z podanym niżej zestawieniem:

- Lata 1994 – 1998 (praca badawczo-rozwojowa *System namierzania radiowego KF p.k. TIEREK- Załącznik nr 5, pkt. II.J, poz. 1*)  
Wykonałem projekt łącza radiowego do przekazywania meldunków o namierzonych nadajnikach radiowych pracujących w paśmie KF bazujący na istniejącym analogowym systemie radioliniowym. Opracowane rozwiązanie zostało zaimplementowane w zautomatyzowanym systemie wykrywania i namierzania sygnałów radiowych KF. Zautomatyzowany system pozwolił na skrócenie czasu reakcji systemu walki radioelektronicznej. System wdrożono w jednostkach walki radioelektronicznej.
- Lata 2000 – 2004 (praca badawczo-rozwojowa *Uniwersalny demodulator cyfrowy dla potrzeb taktycznego systemu walki elektronicznej p.k. PRZEBISNIEG- Załącznik nr 5, pkt. II.J, poz. 2*)  
Opracowałem algorytmy automatycznego rozpoznawania protokołów transmisyjnych stosowanych w kanałach radiowych bazujące na cechach dystynktywnych odbieranego sygnału radiowego oraz ciągu binarnego występującego na wyjściu demodulatora odbiornika rozpoznania radiowego. Opracowane algorytmy zostały wykorzystane w opracowanym przeze mnie module programowym stworzonym w języku wysokiego poziomu C++, który został wykorzystany w Uniwersalnym Demodulatorze Cyfrowym (UDC) przeznaczonym do analizy technicznej, demodulacji i rejestracji sygnałów radiowych w systemach rozpoznania radiowego. UDC umożliwia analizę czasową i widmową sygnałów, pomiar podstawowych parametrów sygnałów radiowych, demodulację sygnałów telegraficznych z manipulacją częstotliwości, fazy oraz demodulację sygnałów zwiłokrotnionych częstotliwościowo i poddanych wtórnej modulacji FM. UDC może analizować sygnały w zakresach UKF. UDC przeznaczony jest do pracy w systemach rozpoznania radiowego. System wdrożono w jednostkach walki radioelektronicznej.
- Lata 2001 – 2003 (praca badawczo-rozwojowa *Zestaw do pomiaru tłumienności traktu radiowego i wyznaczania stref bezpieczeństwa- Załącznik nr 5, pkt. II.J, poz. 3*)  
Opracowałem i wykonałem zestaw nadawczo-odbiorczy do wyznaczania stref bezpieczeństwa dla kancelarii niejawnych. Zestaw umożliwia określanie stref bezpieczeństwa dla miejsc przeznaczonych do instalacji urządzeń teleinformatycznych. Wyniki pomiarów tłumienności łącza radiowego otrzymane za pomocą opracowanego zestawu są niezbędne do certyfikacji kancelarii. Zestaw wdrożono do eksploatacji.

W toku realizacji prac badawczych, w 1998 r., przeprowadzony został mój przewód doktorski (**Załącznik nr 1**). Moim promotorem był dr hab. inż. Grzegorz Różański, a rozprawa pt. *Efektywność kodów splotowych w kanałach zakresu krótkofalowego* uzasadniała tezę pracy mówiącą, że zmodyfikowana metoda Kallela jest najefektywniejszą metodą kodowania i dekodowania korekcyjnego kodów splotowych w kanałach z grupowaniem się błędów.

Głównym celem rozprawy było przedstawienie kompleksowej metody projektowania efektywnego systemu zabezpieczenia transmisji danych przed błędami dla kanału krótkofalowego z wykorzystaniem kodów splotowych. Realizując postawiony cel, w pierwszym etapie pracy przeanalizowałem metody modelowania binarnych kanałów transmisji danych. W efekcie przeprowadzonej analizy, do przebadania wybranego systemu kodowego zabezpieczenia transmisji danych przed błędami oraz do optymalizacji jego parametrów, wybrałem uogólniony model Gilberta kanału ziarnistego. Model ten dobrze odzwierciedla wszystkie cechy rzeczywistego kanału krótkofalowego, cechuje się małą złożonością oraz jest podatny na symulację komputerową.

W części analityczno-przeładowej rozprawy przeanalizowałem na podstawie literatury i usystematyzowałem informacje dotyczące najczęściej spotykanych metod kodowania i dekodowania korekcyjnego kodów splotowych w kanałach z grupowaniem się błędów oraz dokonałem ich porównania. Jako metodę najbardziej efektywną spośród analizowanych, umożliwiającą osiągnięcie dużej wierności transmisji danych (mierzonej wynikową bitową stopą błędów na wyjściu dekodera), przy małym czasie opóźnienia wprowadzanym przez dekodery, wybrałem metodę Kallela. Metoda Kallela dekodowania kodów splotowych wykorzystuje metodę rozpraszania paczek błędów występujących w kanale ziarnistym, polegającą na opóźnieniu względem siebie dwóch przebitych sekwencji kodowych niosących tą samą zakodowaną informację. Pomimo wystąpienia paczki błędów metoda ta umożliwia poprawne zdekodowanie nadanej informacji za pomocą niezakłóconej przebitej sekwencji kodowej.

W rozprawie zaproponowałem modyfikacje metody Kallela polegające na:

- skróceniu okresu wyważania metryk ścieżek odpowiadających zakłóconym paczką błędów bitom kodowym,
- zastosowaniu dodatkowego układu wykrywania paczek błędów.

Otrzymane dane statystyczne z przeprowadzonych symulacji komputerowych pracy kanałów kodowych, w których skład wchodziły dekodery z proponowanymi modyfikacjami, umożliwiły precyzyjne porównanie efektywności dekodowania kodów splotowych przy pomocy zmodyfikowanej metody Kallela i klasycznej metody Kallela. Programy symulacyjne opracowałem w języku programowania wysokiego poziomu C. Najlepszą spośród badanych metod okazała się zmodyfikowana metoda Kallela wykorzystująca skrócony okres wyważania metryk ścieżek.

W rozprawie przedstawiłem również praktyczną metodę określania parametrów zmodyfikowanego dekodera Kallela, zapewniających efektywną korekcję błędów występujących w danym kanale ziarnistym. Wykazałem, że wartości tych parametrów zależą w dużym stopniu od właściwości kanału ziarnistego (parametrów uogólnionego modelu Gilberta).

Z przeprowadzonych w rozprawie analiz wynika, że proponowana zmodyfikowana metoda kodowania i dekodowania korekcyjnego Kallela może być wykorzystana w kanałach z grupowaniem się błędów. Można ją wykorzystać w aplikacjach wymagających małych wartości wprowadzanych czasów opóźnień dekodowania.

Działalność w zakresie systemów radiokomunikacyjnych oraz poprawy wierności transmisji danych w kanałach łączności radiowej musiałem ograniczyć na skutek zmian organizacyjnych zachodzących na Wydziale Elektroniki WAT. Badania w powyższym zakresie zaowocowały opublikowaniem w materiałach konferencyjnych i wygłoszeniem 9-ciu referatów na konferencjach krajowych (**Załącznik nr 5, pkt. II.L, poz. 65÷73**). Wyniki swoich badań opublikowałem ponadto w dwóch opracowaniach wewnętrznych Instytutu Systemów Łączności Wydziału Elektroniki WAT. W tym okresie mojej działalności badawczej powstał przy moim współdziałaniu Uniwersalny Demodulator Cyfrowy. Urządzenie to zostało nagrodzone srebrnym medalem i pucharem na 51 Światowej Wystawie Innowacji, Badań Naukowych i Nowoczesnej Techniki Brussels-Eureka 2002 (**Załącznik nr 8, str. 3**).

W 2005 r. rozpoczynając drugi okres mojej aktywności naukowo-badawczej musiałem ukierunkować się na prace w zakresie kompatybilności elektromagnetycznej, gdyż pojawiła się potrzeba intensyfikacji prac związanych z organizacją w strukturze Wydziału Elektroniki WAT akredytowanego Laboratorium Kompatybilności Elektromagnetycznej (LAB KEM). Jestem zaangażowany w proces organizacji powyższej komórki organizacyjnej od początku jej powołania. W roku 2005 zostałem wyznaczony na stanowisko zastępcy kierownika ds. technicznych, a w roku 2007 objąłem stanowisko kierownika laboratorium, którą to funkcję pełnię do dziś. Od momentu powołania LAB KEM prowadzę badania w zakresie kompatybilności elektromagnetycznej oraz ochrony informacji przed ułotem elektromagnetycznym. Mimo dużego zaangażowania w działalność kierowaną przeze mnie

laboratorium oraz prace z zakresu kompatybilności elektromagnetycznej nie zaniechałem swojego rozwoju w pierwotnym kierunku swoich zainteresowań jakim są systemy radiokomunikacyjne. Równocześnie z pracami z zakresu kompatybilności elektromagnetycznej aktywnie uczestniczę w realizacji prac z zakresu radiokomunikacji oraz z zakresu ochrony informacji przed ulotem elektromagnetycznym. Z racji dużej bliskości tematycznej powyższych obszarów w toku większości realizowanych przeze mnie prac naukowo-badawczych niejednokrotnie korzystałem jednocześnie z wiedzy zaczerpniętej z wszystkich powyższych obszarów.

Moja działalność naukowa w dziedzinie radiokomunikacji, kompatybilności elektromagnetycznej oraz ochrony informacji przed ulotem elektromagnetycznym rozwijała się zgodnie z podanym niżej zestawieniem (**Załącznik nr 5, pkt. II.J, poz. 4÷14**):

- Rok 2006 (*Certyfikat akredytacji laboratorium badawczego Nr AB 693, z dnia 27.02.2006 r.*)  
Przy moim współudziale Laboratorium Kompatybilności Elektromagnetycznej uzyskało akredytację Polskiego Centrum Akredytacji na przeprowadzanie badań urządzeń elektronicznych w zakresie kompatybilności elektromagnetycznej. *Za opracowanie infrastruktury technicznej komory bezodbiciowej oraz procedur badawczych dla akredytowanego Laboratorium Kompatybilności Elektromagnetycznej Wydziału Elektroniki WAT* zostałem uhonorowany w 2006 r. zespołową nagrodą rektorską (**Załącznik nr 8, str. 5**).
- Lata 2006 – 2008 (Grant Rektorski nr 581 *Model mikrotelefonu do skrytej autoryzacji korespondenta radiowego w wojskowych radiostacjach pola walki KF/UKF*)  
Zespół, w którego skład wchodziłem opracował mikrotelefon *do skrytej autoryzacji korespondenta radiowego w wojskowych radiostacjach pola walki KF/UKF*. W ramach powyższego projektu opracowałem moduł programowy odpowiedzialny za poprawę wierności transmisji danych. Powyższe rozwiązanie zostało nagrodzone szeregiem wyróżnień krajowych i międzynarodowych. Do najważniejszych wyróżnień należy zaliczyć złoty medal z wyróżnieniem w 56 Międzynarodowym Konkursie Innowacji „Brussels Eureka 2007” oraz dyplom Ministra Nauki i Szkolnictwa Wyższego (2008 r.) (**Załącznik nr 8, str. 6 i 11**).
- Rok 2011 (*Certyfikat akredytacji w zakresie obronności i bezpieczeństwa Nr 27/MON/2011, z dnia 03.11.2011 r.*)  
Pod moim kierownictwem LAB KEM aplikowało i uzyskało certyfikat akredytacji w zakresie obronności i bezpieczeństwa na przeprowadzanie badań urządzeń przewidzianych do użytkowania w Siłach Zbrojnych RP.
- Rok 2010 (praca badawczo-rozwojowa PBR/523/2010/WAT *Opracowanie technologii i demonstratora zabezpieczenia systemów teleinformatycznych służb porządku publicznego w aspekcie narażenia na terrorystyczne działania silnych impulsów elektromagnetycznych*)  
Celem projektu było przeprowadzenie badań elementów systemu łączności oraz urządzeń informatycznych, narażonych w wyniku ataku terrorystycznego z użyciem ekstremalnie wysokomocowych impulsów elektromagnetycznych oraz opracowanie metod i narzędzi dla przeciwdziałania niszczącemu oddziaływaniu tych impulsów na wybrane składniki takich urządzeń. W ramach projektu brałem udział: w budowie stanowiska badawczego, w badaniach odporności urządzeń łączności na oddziaływanie wysokomocowych impulsów elektromagnetycznych, opracowaniu sprawozdań z badań oraz analizie wyników.
- Lata 2010 – 2012 (praca badawczo-rozwojowa PBR/15-518/2010/WAT *Opracowanie metodologii projektowania i modeli bezpiecznych elektromagnetycznie obudów umożliwiających implementację komputerów przenośnych (typu LAPTOP) i innych służących do przetwarzania danych stanowiących tajemnicę służbową i państwową*)

W ramach projektu opracowałem kompleksowe narzędzia w formie metod pomiaru oraz symulacji komputerowej skuteczności ekranowania obudów ekranujących o gabarytach mniejszych niż  $1,5\text{ m} \times 1,5\text{ m} \times 1,5\text{ m}$  oraz tłumienności wnoszonej przez filtry sieciowe i sygnałowe, które mogą być wykorzystane w procesie weryfikacji poprawności działania wykorzystanych zabezpieczeń urządzeń informatycznych.

- Lata 2010 – 2013 (praca A-0935-RT-GC, Defence R&T Joint Investment Programme on Force Protection A-0120-RT-GC *Intelligent Control of Adversary Radio-communication ICAR*)  
Celem projektu była budowa bezzałogowego naziemnego pojazdu wyposażonego w zautomatyzowany radiowy system zakłócający. W ramach projektu brałem udział w opracowaniu analiz oraz badaniach kompatybilności elektromagnetycznej urządzeń nadawczo-odbiorczych zainstalowanych na mobilnej platformie systemu ICAR.
- Lata 2011 – 2013 (praca PBG/12-604/2011/WAT *Opracowanie i analiza wielopasmowej anteny pracującej w pasmach częstotliwości 2.4 GHz oraz 5.8 GHz wykonanej w technice mikropaskowej*)  
Jako kierownik projektu byłem inicjatorem jego powstania oraz nadzorowałem merytorycznie jego realizację. Opracowałem projekt stanowiska laboratoryjnego do pomiaru parametrów anteny mikropaskowej pracującej w pasmach częstotliwości 2.4 GHz oraz 5.8 GHz. Przy pomocy zestawionego stanowiska laboratoryjnego wykonałem pomiary parametrów wykonanej anteny mikropaskowej oraz przeanalizowałem wyniki pomiarów.
- Rok 2012 (praca DNISW/U/2/BN/1.11/2010/773 *Opracowanie stanowiska pomiarowego oraz procedury badawczej do oceny skuteczności metod zabezpieczeń przed podsłuchem laserowym oraz wykonanie sprzętowego demonstratora technologii*)  
Jako kierownik projektu byłem inicjatorem jego powstania oraz nadzorowałem merytorycznie jego realizację. W ramach pracy powstało stanowisko pomiarowe oraz procedury badawcze do oceny skuteczności metod zabezpieczeń przed podsłuchem laserowym.
- Lata 2012 – 2015 (praca badawczo-rozwojowa 0024/R/ID2/2012/02 *System platformy pomiarowej dla potrzeb bezpieczeństwa informacji stworzony z wykorzystaniem interferometrycznej metody pomiaru drgań*)  
Projekt miał na celu stworzenie mobilnych stanowisk pomiarowych przeznaczonych do oceny zagrożeń polegających na możliwości wykorzystania emisji elektromagnetycznej oraz akustycznej nieintencjonalnie generowanych przez urządzenia informatyczne oraz personel do odtworzenia przez nieupoważnione osoby przetwarzanej informacji. W ramach projektu wykonałem oceny wpływu środowiska na tłumienność sygnałów dla warunków idealnych i rzeczywistych ze szczególnym uwzględnieniem wpływu zakłóceń środowiskowych na sygnały elektromagnetyczne.
- Lata 2013 – 2015 (praca badawczo-rozwojowa DOBR-BIO4/016/13071/2013 *Projekt budowy zabezpieczeń infrastruktury krytycznej w zakresie przetwarzania, magazynowania i przesyłu danych odpornych na działania wysokoenergetycznego promieniowania elektromagnetycznego*)  
Projekt miał na celu wykonanie projektu zabezpieczeń infrastruktury krytycznej w zakresie przetwarzania, magazynowania i przesyłu danych przed skutkami oddziaływania wysokoenergetycznego promieniowania elektromagnetycznego. W ramach projektu przeprowadziłem analizę potencjalnych źródeł wysokoenergetycznych pól elektromagnetycznych i ich możliwości oddziaływania na infrastrukturę telekomunikacyjną. Brałem udział w opracowaniu metodologii pomiarowych dotyczących zjawisk związanych z wysokoenergetycznym promieniowaniem elektromagnetycznym.
- Lata 2014 – 2016 (praca DNISW/U/2/BN/2.4/2014/497 (PBU/02-164/2014/WAT) *Opracowanie sprzętowego demonstratora technologii terminala steganografii akustycznej wykorzystującego model psychoakustyczny p.k. TERMINAL*)



Swój wkład w zakresie poprawy wierności transmisji wniosłem do opracowania sprzętowego demonstratora technologii terminala steganografii akustycznej wykorzystującego model psychoakustyczny. W ramach powyższego projektu opracowałem moduł programowy odpowiedzialny za poprawę wierności transmisji danych. W 2017 r. wraz z zespołem realizującym powyższe urządzenie zostałem wyróżniony nagrodą rektorską *Za opracowanie sprzętowego demonstratora technologii terminala steganografii akustycznej wykorzystującego model psychoakustyczny (Załącznik nr 8, str. 15).*

- Lata 2014 – 2016 (praca DNiSW/U/3/BN/2.5/2014/498 (PBU/02-165/2014/WAT) *Opracowanie sprzętowego demonstratora technologii stanowiska do monitorowania nieautoryzowanych urządzeń/sieci bezprzewodowych Wi-Fi standardu IEEE 802.11 p.k. Wi-Fi)*

Celem projektu było stworzenie stacji namierzania punktów dostępowych Wi-Fi. W ramach projektu przeprowadziłem badania z zakresu kompatybilności elektromagnetycznej opracowanego w ramach projektu urządzenia.

- Lata 2015 – aktualnie (praca badawczo-rozwojowa DOB-1-4/1/PS/2014 *Infrastruktura badawcza w zakresie nowych technologii związanych z generatorami do wytwarzania wysokomocowych impulsów promieniowania elektromagnetycznego, anten nadawczych impulsów HPM, HPRF, RFDF, technologii materiałowych z ochroną i obroną aparatury pomiarowej)*

Projekt miał na celu wykonanie infrastruktury badawczej w zakresie nowych technologii związanych z generatorami do wytwarzania wysokoenergetycznego promieniowania elektromagnetycznego. Produktem realizacji projektu jest komora bezodbiciowa wraz ze stanowiskami badawczymi przeznaczonymi do testów oddziaływania wysokoenergetycznego promieniowania elektromagnetycznego na obiekty badań. Jako kierownik grupy zadań nadzorowałem merytorycznie realizację zadań wykonywanych przez Wojskową Akademię Techniczną. W ramach projektu opracowałem założenia na budowę komory bezodbiciowej oraz koncepcję metodologii pomiaru oraz budowy stanowisk laboratoryjnych przeznaczonych do badania: własności elektrycznych i magnetycznych materiałów będących w stanie sproszkowanym, parametrów materiałów i kompozytów ekranujących w funkcji mocy wysokoenergetycznego promieniowania elektromagnetycznego oraz odporności urządzeń sieci teleinformatycznych na oddziaływanie broni wiązkowej generującej wysokoenergetyczne promieniowanie elektromagnetyczne.

- Lata 2017 – aktualnie (praca badawczo-rozwojowa DOB-1-3/1/PS/2014 *Metody i sposoby ochrony i obrony przed impulsami HPM, w tym zadanie pt. Opracowanie koncepcji budowy przenośnego miernika wysokomocowych pól elektromagnetycznych)*

Projekt miał na celu opracowanie przenośnego miernika wysokomocowych pól elektromagnetycznych. W ramach projektu opracowałem stanowiska laboratoryjne do badań komponentów elektronicznych wykorzystanych w budowie miernika wysokomocowych pól elektromagnetycznych.

Od 2009 r. do chwili obecnej jestem członkiem (z prawem głosu) Komitetu Technicznego KT-104 PKN ds. Kompatybilności Elektromagnetycznej odpowiedzialnego za wprowadzanie na terytorium Polski dokumentów standaryzacyjnych z zakresu kompatybilności elektromagnetycznej.

Od 2012 r. do chwili obecnej jestem zaangażowany w prace dwóch organizacji wspierających rozwój kompatybilności elektromagnetycznej na terenie naszego kraju. Pierwszą z nich jest Sekcja Kompatybilności Elektromagnetycznej Komitetu Elektroniki i Telekomunikacji PAN, w której pełnię funkcję eksperta. Druga instytucja to Polskie Centrum Akredytacji, w której pełnię funkcję audytora technicznego oceniającego pracę laboratoriów badawczych i wzorcujących oraz eksperta technicznego oceniającego pracę jednostek cer-

tyfikujących wyroby oraz jednostek notyfikowanych w obszarze dyrektywy kompatybilności elektromagnetycznej.

W zakresie działalności normalizacyjnej od 2010 r. aktywnie współpracuję z Wojskowym Centrum Normalizacji Jakości i Kodyfikacji (WCNJK). W ramach współpracy z WCNJK w roku 2010 kierowałem pracami zespołu autorskiego opracowującego dwie nowe normy obronne *NO-06-A500: Kompatybilność elektromagnetyczna. Procedury badań zaburzeń elektromagnetycznych i odporności na narażenia elektromagnetyczne* (Załącznik nr 5, pkt. II.J, poz. 16) oraz *NO-06-A200: Kompatybilność elektromagnetyczna. Procedury badań zaburzeń elektromagnetycznych i odporności na narażenia elektromagnetyczne* (Załącznik nr 5, pkt. II.J, poz. 15). Natomiast w roku 2013 kierowałem pracami zespołu autorskiego opracowującego normę obronną *NO-06-A218-4: Technika wojskowa. Warunki Środowiskowe. Część 4: Elektryczne i elektromagnetyczne oddziaływania środowiskowe* (Załącznik nr 5, pkt. II.J, poz. 17). Dodatkowo do chwili obecnej byłem autorem około 36 opinii nowych wydań dokumentów standaryzacyjnych (Załącznik nr 5, pkt. III.M).

Rezultatem prac naukowo-badawczych w dziedzinie radiokomunikacji, kompatybilności elektromagnetycznej oraz ochrony informacji przed ulotem elektromagnetycznym jest dorobek publikacyjny zawierający oprócz monografii (Załącznik nr 4): 45 artykułów naukowych (Załącznik nr 5, pkt. II.A, poz. 1÷7 oraz pkt. II.E, poz. 1÷38), w tym 7 opublikowanych w periodykach naukowych z *Listy Filadelfijskiej (Elektronika IR Elektrotechnika - 2, Advances in Engineering Software – 1 i Electrical Review – 4)*, 99 referatów konferencyjnych (Załącznik nr 5, pkt. II.L, poz. 1÷99).

Moją działalność publikacyjną opisują niżej wymienione wartości parametrów:

- sumaryczny Impact Factor według listy Journal Citation Reports (JCR): IF = 4,106 (Załącznik nr 11, str. 2),
- liczba cytowań publikacji według bazy Web of Science: 132 (Załącznik nr 9, str. 2),
- liczba cytowań publikacji według bazy Scopus: 380 (Załącznik nr 10, str. 2),
- Indeks Hirsha według bazy Web of Science: h = 7 (Załącznik nr 9, str. 2),
- Indeks Hirsha według bazy Scopus: h = 12 (Załącznik nr 10, str. 2).

## 6. Literatura

- [1] Araneo R., Celozzi S., Lovat G.: *Electromagnetic shielding*, John Wiley & Sons, INC., New Jersey, 2008.
- [2] Arendarski J.: *Niepewność pomiarów*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa, 2006, ISBN 83-7207-653-7.
- [3] Asmanis G.: *Measurement and modeling of EMI filters high frequency parasitic parameters*, Riga Technical University, Faculty of Power and Electrical Engineering, Institute of Industrial Electronics and Electrical Engineering, Riga 2014.
- [4] Bugaj M., Nowosielski L., Piwowarczyk K., Przesmycki R., Wnuk M.: *Analysis of the Radiated Emissions of IT Equipment*, Proceedings of PIERS 2012, Moscow, 2012, s. 1419–1423, ISSN 1599-9450, ISBN 978-1-934142-22-6.
- [5] Bugaj M., Nowosielski L., Piwowarczyk K., Przesmycki R., Wnuk M.: *Methods of Measuring Shielding Effectiveness of Small Shielded Chambers*, Proceedings of PIERS, Moscow, 2012, s. 1437–1442, ISSN 1599-9450, ISBN 978-1-934142-22-6.
- [6] Bugaj M., Nowosielski L., Przesmycki R., Wnuk M.: *Analysis of conducted and radiated emission from IT devices in the frequency band 0,15 MHz – 6000 MHz*, Mediterranean Microwave Symposium (MMS), Hammamet, Tunezja, 2011, IEEE Xplore, ISSN 2157-9822, ISBN 978-1-4577-1814-4.
- [7] Bugaj M., Nowosielski L., Przesmycki R., Wnuk M.: *The laptop casing shielding effectiveness measurement*, Mediterranean Microwave Symposium (MMS), Hammamet, Tunezja, 2011, IEEE Xplore, ISSN 2157-9822, ISBN 978-1-4577-1814-4.
- [8] DA-05, *Polityka dotycząca uczestnictwa w badaniach biegłości*, Polskie Centrum Akredytacji, Wydanie 6, Warszawa, 22.04.2016 r.
- [9] Drinovsky J.: *Insertion Loss Estimation of EMI Filters in Unmatched Input/Output Impedance System*, RADIOENGINEERING, Vol. 20, Nr 1, 2011.
- [10] Dyrektywa 2014/30UE Parlamentu Europejskiego i Rady, z dnia 26.02.2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do kompatybilności elektromagnetycznej.
- [11] EA-4/02, *Wyrażanie niepewności pomiaru przy wzorcowaniu*, Główny Urząd Miar, 2001.
- [12] EN 55022:2000, *Information technology equipment – Radio disturbance characteristics – Limits and methods of measurement*.
- [13] EN 55022:2010/AC:2011, *Information technology equipment – Radio disturbance characteristics – Limits and methods of measurement*.
- [14] EN 55032:2015-09, *Kompatybilność elektromagnetyczna urządzeń multimedialnych - Wymagania dotyczące emisji*.
- [15] ESCC Basic Specification No. 24400, *Measurement of insertion loss for EMI suppression filters*, European Space Agency, Issue 2, 2013.
- [16] Faez R., Martin I.M., Rezende M. C.: *Radar Cross Section Measurement (8-12 GHz) of Magnetic and Dielectric Microwave Absorbing Thin Sheets*, Revista de Fisica Aplicadae Instrumentacao, Vol. 15, Nr 1, 2002, s. 24-29.
- [17] Frankland R., Wolthusen S.: *Electronic surveillance through the exploitation of compromising emanations*, Royal Holloway Series, 2011.
- [18] Fukunaga K., Tosaka T., Yamanaka Y.: *Method for determining whether or not information is contained in electromagnetic disturbance radiated from a PC display*, IEEE Transactions on Electromagnetic Compatibility, Vol. 53, Nr 12, 2011, s. 318-324.
- [19] Gonschorek K. H., Vick R.: *Electromagnetic compatibility for device design and system integration*, Springer, New York, 2009.

- [20] Grzesiak K., Kubiak I., Musiał S., Przybysz A.: *Elektromagnetyczne bezpieczeństwo informacji*, Wojskowa Akademia Techniczna, Warszawa, 2009, ISBN 978-83-61486-32-9.
- [21] Grzesiak K., Kubiak I., Musiał S., Przybysz A.: *Generator rastra w procesie infiltracji elektromagnetycznej*, Wojskowa Akademia Techniczna, Warszawa, 2012, ISBN 978-83-62954-28-5.
- [22] IEEE Std 299.1:2013, *IEEE Standard Method for Measuring the Shielding Effectiveness of Enclosures and Boxes Having all Dimensions between 0,1 m and 2 m*.
- [23] ISO/IEC 43-1, *Proficiency testing by interlaboratory comparison – Part 1: Development and operation of proficiency testing schemes*, ISO/IEC, Geneva, 1997.
- [24] Khun M. G.: *Compromising emanations of LCD TV Sets*, IEEE Transactions on Electromagnetic Compatibility, Vol. 55, Nr. 3, 2013, s. 564-570.
- [25] Knott F., Shaeffer F., Tuley T.: *Radar cross section. Second edition*, SCITECH Publishing, INC, 2004.
- [26] Krawczak R., Nowosielski L.: *Opis techniczny i instrukcja obsługi miernika natężenia pola elektromagnetycznego*, Instytut Systemów Łączności, WAT, 2001.
- [27] Krawczak R., Nowosielski L.: *Opis techniczny i instrukcja obsługi nadajnika sygnału pomiarowego*, Instytut Systemów Łączności, WAT, 2001.
- [28] Markus G. Kuhn: *Compromising emanations: Eavesdropping risks of computer displays. Technical Report UCAM-CL-TR-577*, University of Cambridge, 2003, ISSN 1476-2986.
- [29] Montrose M. I., Nakauchi E. M.: *Testing for EMC compliance*, John Wiley & Sons, INC., New Jersey, 2004.
- [30] Morgan D.: *A Handbook for EMC Testing and Measurement, The Institution of Engineering and Technology*, London, United Kingdom, 2007, ISBN: 978-0-86341-756-6.
- [31] NATO, *SDIP-27/1 – NATO TEMPEST Requirements and Evaluation Procedures*.
- [32] NATO, *SDIP-28/1 – NATO Zoning Procedures*.
- [33] Nowosielski L., Łopatka J.: *Measurement of Shielding Effectiveness with the Method Using High Power Electromagnetic Pulse Generator*, PIERS 2014 Conference Proceedings, Guangzhou, China, 2014, s. 2727–2731, ISSN 1559-9450.
- [34] Nowosielski L., Orliński B.: *Krajowe badania międzylaboratoryjne – Pomiary emisyjności w zakresie zaburzeń promieniowanych w paśmie częstotliwości od 30 MHz do 1 GHz*, VI Krajowe Warsztaty Kompatybilności Elektromagnetycznej, Wrocław, 2007.
- [35] Nowosielski L., Przesmycki R., Wnuk M.: *Analiza poziomów emisji promieniowanej współczesnych urządzeń informatycznych w paśmie 30 MHz - 6000 MHz*, KKRRiT, Kraków, 2010, Przegląd Telekomunikacyjny, Nr 6/2010, s. 384–387, ISSN 1230-3496.
- [36] Nowosielski L., Przesmycki R., Wnuk M.: *Analiza poziomów emisji przewodzonej na zaciskach zasilania współczesnych urządzeń informatycznych w paśmie 0,15 MHz - 30 MHz*, KSTiT, Wrocław, 2010, Przegląd Telekomunikacyjny, Nr 8–9/2010, s. 1577–1583, ISSN 1230-3496.
- [37] Nowosielski L., Przesmycki R., Wnuk M.: *Measurement of conducted emissions from military equipment in accordance with the NO-06-A500 standard*, 19<sup>th</sup> International Wrocław Symposium and Exhibition on EMC, 2008.
- [38] Nowosielski L., Przesmycki R., Wnuk M.: *Measurement of radiated emissions from military equipment in accordance with the NO-06-A500 standard*, 19<sup>th</sup> International Wrocław Symposium and Exhibition on EMC, 2008.
- [39] Nowosielski L., Przesmycki R., Wnuk M.: *Metodologia pomiaru absorpcji materiałów z wykorzystaniem generatora HPEM*, Przegląd Telekomunikacyjny, Nr 8–9/2014, s. 821–827, ISSN 1230-3496.

- [40] Nowosielski L., Przesmycki R., Wnuk M.: *Pomiar emisji promieniowanej emitowanej przez urządzenia wojskowe*, Przegląd Telekomunikacyjny, Zeszyt nr 8–9, s. 1347, 2008.
- [41] Nowosielski L.: *Urządzenie do projektowania i pomiaru tłumienności filtrów sieciowych i sygnałowych (dokumentacja techniczna i eksploatacyjna)*, Warszawa, 2017.
- [42] Nowosielski L., Wnuk M.: *Compromising Emanations from USB 2 Interface*, PIERS 2014 Conference Proceedings, 25-28.08.2014 r., Guangzhou, China, s. 2706-2710, ISSN 1559-9450.
- [43] Nowosielski L., Wnuk M.: *Implementation of Universal RF-shielded Enclosure for IT Equipment Protection*, 36<sup>th</sup> Progress in Electromagnetics Research Symposium, Prague, Czech Republic, 2015, s. 317–320, ISBN 978-1-934142-30-1.
- [44] Nowosielski L., Wnuk M.: *Pomiar efektywności ekranowania*, Przegląd Elektrotechniczny, Nr 3/2015, s. 81–84, ISSN 0033-2097.
- [45] Nowosielski L., Wnuk M., Ziółkowski C.: *Interlaboratory Tests in Scope of Measurement of Radio Disturbance*, European Microwave Week, Rzym, 2009.
- [46] NO-06-A500:2012, *Kompatybilność elektromagnetyczna. Procedury badań zaburzeń elektromagnetycznych i odporności na narażenia elektromagnetyczne*, Wojskowe Centrum Normalizacji Jakości i Kodyfikacji.
- [47] NO-06-A501:2009/A1:2017, *Kompatybilność elektromagnetyczna. Tłumienność obiektów ekranujących. Metody badań*. Wojskowe Centrum Normalizacji Jakości i Kodyfikacji.
- [48] NO-19-A504:2011, *Uzbrojenie i sprzęt wojskowy. Tłumienność ekranujących konstrukcji okrętowych. Metody badań*. Wojskowe Centrum Normalizacji Jakości i Kodyfikacji.
- [49] PN-EN ISO/IEC 17025:2018-02, *Ogólne wymagania dotyczące kompetencji laboratoriów badawczych i wzorcujących*, Polski Komitet Normalizacyjny.
- [50] PN-EN ISO/IEC 17043:2011, *Ocena zgodności – Ogólne wymagania dotyczące badania biegłości*, Polski Komitet Normalizacyjny.
- [51] PN-EN-50147-1:2000, *Kompatybilność elektromagnetyczna (EMC). Komory bezodbiwoe. Pomiar tłumienności ekranu*. Polski Komitet Normalizacyjny.
- [52] PN-EN 55016-4-2:2011/A1:2014-10, *Wymagania dotyczące aparatury pomiarowej i metod pomiaru zaburzeń radioelektrycznych oraz odporności na zaburzenia – Część 4-2: Niepewności, statystyka i modelowanie poziomu dopuszczalnego – Niepewność aparatury pomiarowej*. Polski Komitet Normalizacyjny.
- [53] *Raport techniczny z realizacji projektu badawczo-rozwojowego nr OR00000511, Umowa z MNiSW Nr: 0005/R/T00/2010/11, Wykonanie modeli obudów, Zadanie nr XI, Tom I*, Warszawa, 2012.
- [54] *Raport techniczny z realizacji projektu badawczo-rozwojowego nr OR00000511, Umowa z MNiSW Nr: 0005/R/T00/2010/11, Wykonanie modeli obudów, Zadanie nr XI, Tom II*, Warszawa, 2012.
- [55] Ruszel P.: *Kompatybilność elektromagnetyczna elektronicznych urządzeń pomiarowych*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław, 2008, ISBN 978-83-7493-423-7.
- [56] Rybicki T., Brzeziński S., Karbownik I., Śledzińska K., Krawczyńska I.: *Usability of a modified method for testing emissivity to assess the real shielding properties of textiles*, Fibres Text. East. Eur. 2010, Vol. 18, Nr 5 s. 76-80, ISSN: 1230-3666.
- [57] Rybicki T., Stempień Z., Rybicki E., Szugajew L.: *EMI shielding effectiveness of polyacrylonitrile fabric with polyaniline deposition by reactive inkjet printing and model approach*, IEEE Transactions on Electromagnetic Compatibility, Vol. 58, Nr 4, 2016.
- [58] Schaffner EMC Systems Ltd.: *EMC Measurement Uncertainty*, 2002.

- [59] Sroka J.: *Niepewność pomiarowa w badaniach EMC. Pomiary emisyjności radioelektrycznej*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa, 2009, ISBN 978-83-7207-837-7.
- [60] Tao G., Wang Q.: *Research on Arch Method for Testing the Absorbing Capability of Absorbing Materials*, Proceedings of PIERS, Beijing, 2009, s. 244–248.
- [61] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U. 2010, Nr 182, poz. 1228.
- [62] Valouch J., Kovář S., Kadavý T., Pospíšilík M., Adánek M.: *Enclosure shielding effectiveness calculation using SHADE algorithm*, 2018 19<sup>th</sup> International Scientific Conference on Electric Power Engineering (EPE), IEEE Xplore, 2018, s. 1-4, DOI: 10.1109/EPE.2018.8396021.
- [63] Vuagnoux M., Pasini S.: *An improved technique to discover compromising electromagnetic emanations*, 2010 IEEE International Symposium on Electromagnetic Compatibility, Fort Lauderdale, FL, USA, 2010, s. 121-126, DOI:10.1109/IEMC.2010.5711257.
- [64] Wang L., Yu B.: *Analysis and Measurement on the Electromagnetic Compromising Emanations of Computer Keyboards*, Seventh International Conference on Computational Intelligence and Security, 2011 s. 640-643.
- [65] Wang L., Yu B.: *Research on the Compromising Electromagnetic Emanations of PS/2 Keyboard*, Proceedings of the 2012 International Conference on Communication, Electronics and Automation Engineering, 2012, s. 23-31.
- [66] Wang S., Qiu Y., Tian J.: *Research on Shielding Effectiveness Test of Bulkhead in a Compartment Shelter*, IEEE Transactions on Electromagnetic Compatibility, 2018, s. 1-4, DOI: 10.1109/TEMC.2018.2801307.
- [67] Williams T, *EMC for product designers*, Elsevier Ltd., Burlington, 2007.
- [68] Zahra K., Aliakbarian H.: *Wideband full wave shielding effectiveness simulation of structures with wire grid meshes*, 2017 International Symposium on Electromagnetic Compatibility - EMC EUROPE, IEEE Xplore, Angers, France, 2017, s. 1-4, DOI: 10.1109/EMCEurope.2017.8094742.
- [69] Zbojovský J., Pavlík M., Kruželák L., Kostelec M.: *Influence of shielding paint on the combination of building materials for evaluation of shielding effectiveness*, 2018 19<sup>th</sup> International Scientific Conference on Electric Power Engineering (EPE), IEEE Xplore, Brno, Czech Republic, 2018, s. 1-4, DOI: 10.1109/EPE.2018.8395941.
- [70] Zhou C., Gui L.: *Shielding effectiveness measurement of small size metal enclosure*, 2016 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC), IEEE Xplore, Shenzhen, China, 2016, s. 417-419, DOI: 10.1109/APEMC.2016.7522755.
- [71] Zhou H., Yan L., Fang M., Zhao X., Qiang Liu Q.: *Shielding effectiveness prediction of metallic structures with thin slots using FDTD*, 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), IEEE Xplore, 2018, s. 359-362, DOI: 10.1109/IEMC.2018.8393798.

Nowosielski L.

.....  
dr inż. Leszek Nowosielski