Załącznik nr 1

AUTOREFERAT

dr inż. Ireneusz Kubiak

Wojskowy Instytut Łączności
im. prof. dr. hab. Janusza Groszkowskiego

Zegrze Południowe, kwiecień 2020 r.

Spis treści

1. DANE HABILITANTA 3

2. POSIADANE DYPLOMY, STOPNIE NAUKOWE LUB ARTYSTYCZNE – Z PODANIEM PODMIOTU NADAJĄCEGO STOPIEŃ, ROKU ICH UZYSKANIA ORAZ TYTUŁU ROZPRAWY DOKTORSKIEJ 3

3. INFORMACJE O DOTYCHCZASOWYM ZATRUDNIENIU W JEDNOSTKACH NAUKOWYCH 3

4. OMÓWIENIE OSIĄGNIĘĆ, O KTÓRYCH MOWA W ART. 219 UST. 1 PKT. 2 USTAWY z dn. 20 LIPCA 2018 r. PRAWO O SZKOLNICTWIE WYŻSZYM I NAUCE (DZ.U. z 2018 r., poz. 1669) 4
   4.1. Tytuł osiągnięcia naukowego 4
   4.2. Omówienie celu naukowego wskazanej publikacji i osiągniętych wyników wraz z omówieniem ich ewentualnego wykorzystania 4

LITERATURA 26

5. INFORMACJA O WYKAZYWANIU SIĘ ISTOTNĄ AKTYWNOŚCIĄ NAUKOWĄ ALBO ARTYSTYCZNĄ REALIZOWANĄ W WIĘCEJ NIŻ JEDNEJ UCZELNI, INSTYTUCJI NAUKOWEJ LUB INSTYTUCJI KULTURY, W SZCZEGÓLNOŚCI ZAGRANICZNEJ 29
   5.1. Aktywność naukowa do uzyskania stopnia doktora nauk technicznych 29
   5.2. Aktywność naukowa po uzyskaniu stopnia doktora nauk technicznych 30
      5.2.1. Obszar prac niejawnych 30
      5.2.2. Projekty, członkostwo w organizacjach naukowych, współpraca międzynarodowa 31
      5.2.3. Uczestnictwo w programach europejskich oraz innych programach międzynarodowych i krajowych 35
      5.2.4. Udział w konsorcjach i sieciach badawczych 35
      5.2.5. Kierowanie projektami realizowanymi we współpracy z naukowcami z innych ośrodków polskich i zagranicznych oraz we współpracy z przedsiębiorcami 36
      5.2.6. Udział w komitetach redakcyjnych czasopism, radach naukowych oraz międzynarodowych i krajowych organizacjach i towarzystwach naukowych 36

6. INFORMACJA O OSIĄGNIĘCIACH DYDAKTYCZNYCH, ORGANIZACYJNYCH I POPULARYZUJĄCYCH NAUKĘ 37
   6.1. Osiągnięcia dydaktyczne 37
   6.2. Osiągnięcia w zakresie organizacyjnego wsparcia badań naukowych 38
   6.3. Informacja o działalności popularyzującej naukę, udział w zespołach eksperckich i konkursowych, recenzowanie publikacji w czasopismach międzynarodowych i krajowych oraz konferencji międzynarodowych 40
   6.4. Inne osiągnięcia, niewymienione wcześniej 40

7. PODSUMOWANIE DOROBKU NAUKOWO-BADAWCZEGO ORAZ POZOSTAŁYCH OSIĄGNIĘĆ (po uzyskaniu stopnia doktora nauk technicznych) 41

1. IMIĘ I NAZWISKO

Ireneusz KUBIAK

2. POSIADANE DYPLOMY, STOPNIE NAUKOWE LUB ARTYSTYCZNE – Z PODANIEM PODMIOTU NADAJĄCEGO STOPIEŃ, ROKU ICH UZYSKANIA ORAZ TYTUŁU ROZPRAWY DOKTORSKIEJ

a) Dyplom doktora nauk technicznych w zakresie telekomunikacji (załącznik nr 6);
Instytut Telekomunikacji i Akustyki Politechniki Wrocławskiej, 2000 rok;
Tytuł rozprawy: *Identyfikacja przebiegu czasowego pola elektromagnetycznego na podstawie jego pomiaru przy ograniczonym paśmie odbioru*
Promotor: prof. dr hab. inż. Tadeusz Więckowski
Recenzenci: prof. dr hab. inż. Władysław Kołosowski
prof. dr hab. inż. Ryszard Makowski

b) Dyplom magistra matematyki w zakresie zastosowań matematyki (załącznik nr 7);
Wydział Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego, 1993 rok;
Tytuł pracy: *Aproksymacja funkcji ciągłych rzeczywistych i zespolonych w R i C*
Promotor: dr Anna Warzecha

c) Dyplom magistra inżyniera w zakresie *Budowy i eksploatacji systemów łączności*;
Wydział Elektroniki Wojskowej Akademii Technicznej, 1992 rok;
Tytuł pracy: *Analiza sygnałów losowych na wyjściu układów liniowych*;
Promotor: dr hab. inż. Cezary Ziółkowski, prof. WAT

3. INFORMACJE O DOTYCHCZASOWYM ZATRUDNIENIU W JEDNOSTKACH NAUKOWYCH

Nazwa jednostki naukowej	Stanowisko	Okres zatrudnienia
Wojskowy Instytut Łączności	pracownik naukowy – inżynier pracowni zakłóceń elektromagnetycznych zakładu kompatybilności elektromagnetycznej	1992 – 1993
	pracownik naukowy – starszy inżynier pracowni zakłóceń elektromagnetycznych zakładu kompatybilności elektromagnetycznej	1993 – 1997
	kierownik pracowni zakłóceń elektromagnetycznych zakładu kompatybilności elektromagnetycznej	1997 - 2004
	adiunkt – kierownik zakładu kompatybilności elektromagnetycznej	2004 – obecnie
	kierownik laboratorium WIŁ (Laboratorium Kompatybilności Elektromagnetycznej, Laboratorium Badań Środowiskowych, Laboratorium Analiz Ataków Cybernetycznych od roku 2016)	2007 – obecnie

4. OMÓWIENIE OSIĄGNIĘĆ, O KTÓRYCH MOWA W ART. 219 UST. 1 PKT. 2 USTAWY z dn. 20 LIPCA 2018 r. PRAWO O SZKOLNICTWIE WYŻSZYM I NAUCE (DZ.U. z 2018 r., poz. 1669)

4.1. Tytuł osiągnięcia naukowego

Ireneusz Kubiak, Joe Loughry: *Specjalne fonty komputerowe w bezpieczeństwie elektromagnetycznym cyfrowych standardów graficznych. TEMPEST optyczny*, monografia, Wydawnictwo Wojskowej Akademii Technicznej, 2020, liczba stron 380, ISBN 978-83-7938-274-3 (załącznik nr 3)
Recenzenci:
prof. dr hab. inż. Piotr Gajewski (recenzja: załącznik nr 4a)
dr hab. inż. Krzysztof Duda, prof. AGH (recenzja: załącznik nr 4b)
Oświadczenia autorów:
dr inż. Ireneusz Kubiak (załącznik nr 4c)
prof. Joe Loughry (załącznik nr 4d)

4.2. Omówienie celu naukowego wskazanej publikacji i osiągniętych wyników wraz z omówieniem ich ewentualnego wykorzystania

Po uzyskaniu stopnia doktora nauk technicznych w roku 2000, moje prace w obszarze bezpieczeństwa elektromagnetycznego (EM) przetwarzanych informacji uległy znacznemu nasileniu. Wiązało się to ze wzrostem zainteresowania rodzimymi rozwiązaniami technicznych urządzeń specjalnych wykorzystywanych do budowy niejawnych systemów informatycznych. Ponieważ liczba dostępnej literatury, poruszającej aspekty związane z zagrożeniami infiltracji EM oraz rozwiązaniami technicznymi, które mogły zapewnić pełne bezpieczeństwo EM przetwarzanych informacji była niewielka, realizacja postawionego zadania stała się niezmiernie trudna. Po upływie kilkunastu lat od obrony pracy doktorskiej, sytuacja związana z liczebnością specjalistycznej literatury nie uległa znacznej poprawie. Powodów można szukać przede wszystkim w ograniczonej jawności prac zarówno w obszarze przeciwdziałania bezinwazyjnemu pozyskiwaniu informacji, jak i możliwości pozyskiwania danych przy wykorzystaniu zjawisk EM, towarzyszących pracy urządzeń specjalnych.

Szczególnie istotnym aspektem w obszarze ochrony informacji jest przeciwdziałanie procesowi bezinwazyjnego jej pozyskiwania. Zjawiskiem wykorzystywanym w przechwytywaniu informacji jest powstawanie pola EM, gdy informacja ta jest przetwarzana w postaci elektrycznej. Wówczas natężenie pola zmienia się w takt zmian sygnału elektrycznego reprezentującego przetwarzaną informację, przyjmując jego cechy dystynktywne (charakterystyczne). Za cechy dystynktywne uważa się zmiany amplitudy lub struktury bitowej sygnału elektrycznego (zmiana kolorów tła i znaków), związane np. z wyświetlanymi (drukowanymi) danymi na monitorze komputerowym. Odbiór i rejestracja fal EM (tzw. emisji ujawniającej) może pozwolić na odtworzenie informacji, a tym samym wejście w jej posiadanie – w sposób niebudzący podejrzenia – przez osobę przetwarzającą dane [13, 20].

Najbardziej spektakularnym zjawiskiem jest możliwość odtworzenia danych graficznych, gdy źródłem emisji ujawniających są tory graficzne urządzeń informatycznych. Mamy tu na uwadze analogowe, jak i cyfrowe standardy wideo, układy naświetlania bębnów światłoczułych drukarek laserowych oraz wyświetlacze drukarek.

Wówczas odtwarzana informacja przedstawiana jest w postaci obrazów, zawierających czytelne dane [1-3, 5, 21].

Ochrona informacji w niejawnych systemach informatycznych najczęściej kojarzy się z ochroną kryptograficzną. Jednak nie w każdym przypadku ochrona danych może być skutecznie wspierana takimi metodami. Należy zwrócić uwagę, że źródłem promieniowania EM jest nie tylko medium transmisyjne w postaci kabla sygnałowego, który może przesyłać dane zaszyfrowane. Źródłem niepożądanych emisji jest cały tor graficzny, poczynając od karty graficznej, a kończąc na matrycy monitora komputerowego [14, 19, 24-25]. Nie da się więc zaszyfrować sygnału w całym torze. Związane jest to ze specyfiką przetwarzanych informacji graficznych. Są to dane, które mimo zaszyfrowania i występowania w kanele transmisyjnym jako tzw. BLACK, w urządzeniu końcowym muszą występować w postaci jawnej – tzw. RED. Tymi danymi są obrazy wyświetlane na monitorze komputerowym (wyświetlaczu drukarki) czy też drukowane przez drukarki laserowe. Poza tym koszty zabezpieczeń kryptograficznych związane z ochroną, dystrybucją czy też zarządzaniem danymi kryptograficznymi są bardzo duże.

Z punktu widzenia EM ochrony informacji istotne są dwa zagadnienia, których ciągły rozwój, przy nieprzerwanym postępie technologicznym urządzeń informatycznych, zapewnia bezpieczeństwo przetwarzanych danych niejawnych. Jednym z tych zagadnień jest poszukiwanie metod cyfrowego przetwarzania sygnałów i obrazów, które mogą być wykorzystywane w ocenie urządzeń specjalnych czyli w procesie ich certyfikacji [6, 8, 12, 38]. Metody te z oczywistych powodów nie mogą być jawne ponieważ dotyczą zagadnień ściśle związanych z bezpieczeństwem informacji. Dotychczasowe doświadczenie habilitanta pokazuje, że występujące emisje ujawniające od urządzeń teleinformatycznych w wykonaniu specjalnym, charakteryzują się bardzo niskimi poziomami [7, 26-27, 34, 37]. Jakość uzyskiwanych obrazów jest bardzo słaba a analizy wzrokowe tych obrazów stają się niewystarczające. Brak jest możliwości wskazania elementów zawartych w obrazie, istotnych z punktu widzenia prowadzenia procesu infiltracji EM. Konieczne jest poszukiwanie metod wspierających proces decyzyjny. Powodem jest wspomniana słaba jakość obrazów uzyskiwanych z emisji ujawniających. Poszukiwane elementy w takich obrazach maskowane są sygnałami zaburzającymi i wszechobecnymi szumami [31, 45-46]. Niezbędne jest więc poszukiwanie metod, które będą skuteczne w warunkach, jakie występują w procesie infiltracji EM.

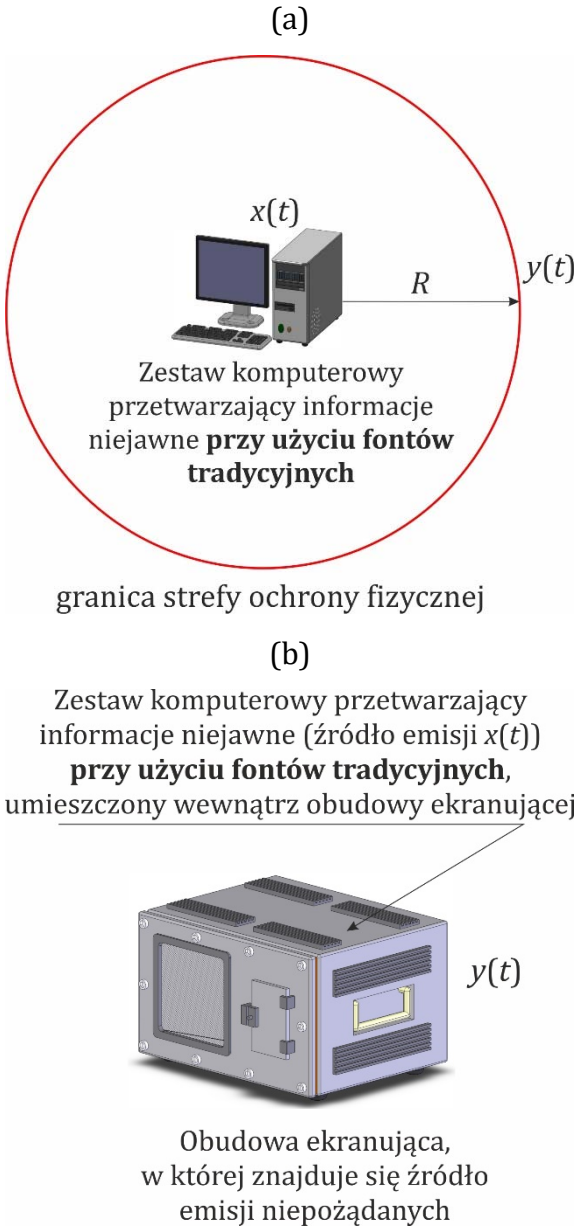
Drugim zagadnieniem jest poszukiwanie rozwiązań minimalizujących powstawanie sygnałów niepożądanych, których cechy dystynktywne mogą świadczyć o ich korelacji z przetwarzaną informacją niejawną. Zjawisku infiltracji EM można przeciwdziałać stosując różnorodne metody w obszarze rozwiązań organizacyjnych, jak i technicznych (rys.1):

- organizacja odpowiednich stref ochrony fizycznej, na granicy których mierzone wartości emisji EM uniemożliwią odtworzenie informacji;
- tłumienie emisji niepożądanych u źródła, czyli stosowanie rozwiązań konstrukcyjnych z zastosowaniem nowoczesnych technologii inżynierii kompatybilności EM.

Metody organizacyjne to przede wszystkim kontrola dostępu do stref ochronnych o odpowiednich promieniach, których wartości określane są zależnościami tłumienia pola EM w różnych środowiskach propagacyjnych (np. otwarta przestrzeń, teren zurbanizowany, pomieszczenia biurowe).

Moje prace skupiają się przede wszystkim na rozwiązaniach technicznych, gdyż takie są oceniane i weryfikowane w kierowanym przeze mnie laboratorium Wojskowego Instytutu Łączności, w oparciu o dokumenty [47-49] oraz posiadane świadectwa uznania

laboratorium przez Agencję Bezpieczeństwa Wewnętrznego i Służbę Kontrwywiadu Wojskowego.



Rys.1. Sposoby ochrony EM informacji przed infiltracją EM: (a) strefowanie, (b) obudowa ekranująca

Powszechnie stosowane rozwiązania techniczne [32-33, 36, 39] nie wpływają bezpośrednio na źródła emisji ujawniających, a jedynie eliminują skutki takich źródeł, czyli obniżają poziomy emisji ujawniających do wartości, które uniemożliwiają odtworzenie przetwarzanych informacji. W tym celu stosowane są m.in. kabiny lub obudowy ekranujące, szyby ekranujące, uszczelki EM, filtry sygnałowe i sieciowe. Takie podejście do istniejącego problemu ochrony informacji przed EM przenikaniem skutkowało powstaniem u schyłku XX wieku pierwszego polskiego komputera tzw. klasy TEMPEST, przeznaczonego do przetwarzania informacji niejawnych [50]. Twórcą tego urządzenia był zespół kierowany przez habilitanta. Jednak takie rozwiązanie urządzeń

klasy TEMPEST[1] z upływem lat zaczęło coraz częściej budzić niezadowolenie użytkowników. Wynikało ono przede wszystkim z masy urządzenia, a także ograniczeń funkcjonalnych. Stosowano specjalne złącza, uniemożliwiające podłączenie innych urządzeń niż dedykowane (np. złącza USB dla myszy komputerowej, drukarki itp.). Występowały ograniczenia w dostępie do napędów dysków HDD oraz płyt CD/DVD. Rozwiązania techniczne, ukierunkowane na obniżenie poziomów emisji niepożądanych do akceptowalnych wartości, wymagają zmian konstrukcyjnych urządzeń a nawet układów elektronicznych. Poprawność zaimplementowanych rozwiązań potwierdzana jest wydaniem stosownego certyfikatu ochrony EM. Wówczas urządzenie informatyczne może być stosowane przez instytucje, które przetwarzają informacje niejawne w rozumieniu Ustawy o ochronie informacji niejawnych [51]. Należy jednak zauważyć, że wysoka cena nabycia takich urządzeń jest barierą ekonomiczną do ich stosowania przez wiele firm. Dodatkowym elementem nieułatwiającym pozyskanie takich urządzeń jest wymóg specjalnej ich ochrony.

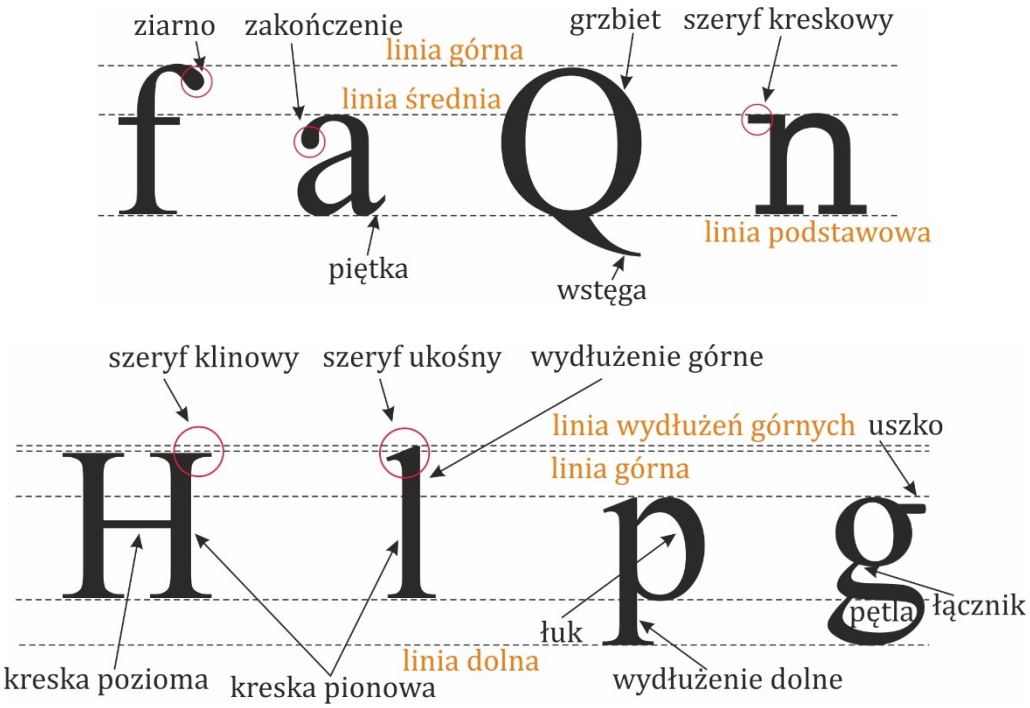
Zjawisko infiltracji EM możliwe jest przede wszystkim ze względu skorelowania emisji ujawniających z przetwarzanymi danymi, w tym konkretnym przypadku danymi graficznymi [15, 17, 35, 40, 42, 44]. Dotychczasowe doświadczenie habilitanta, jak i prowadzone analizy źródeł podatnych na podsłuch EM pokazują, że dla podniesienia poziomu bezpieczeństwa EM informacji można stosować rozwiązania, które będą odpowiednio kształtować źródła emisji wrażliwych. Takie podejście musi wpływać na ograniczenie cech dystynktywnych sygnału pierwotnego, a tym samym skorelowanego z nim sygnału emisji ujawniającej.

Najczęściej przetwarzanymi danymi niejawnymi są dane tekstowe. Do ich przetwarzania wykorzystuje się typowe fonty[2] komputerowe Arial lub Times New Roman, które posiadają wiele cech charakterystycznych – np. zaokrąglenia, wydłużenia dolne i górne liter, oczka, szeryfy, ziarna itp. (rys.2) – ułatwiających ich rozróżnianie. Prowadzone badania graficznych źródeł emisji pokazują, że można podjąć się zaprojektowania fontów komputerowych o kształtach, które po pierwsze będą akceptowalne przez użytkownika, po drugie nie pogorszą znacznie czytelności, a po trzecie – będą odporne na infiltrację EM. Ponadto, należy uwzględnić właściwości Kanału Przenikania Informacji (typu promieniowanego), który posiada cechy filtra górnoprzepustowego. Jest to niezwykle istotna właściwość, która ma duży wpływ na postacie znaków fontów odtwarzanych na bazie rejestrowanych emisji ujawniających. Znaki te identyfikowane są tylko poprzez krawędzie pionowe i ukośne (analogowy standard VGA [9-11, 16], rys.3a). Wypełnienia mogą pojawić się w przypadku cyfrowego standardu wideo, co wynika z zastosowanego algorytmu kodowania kolorów (ang. *Transition Minimized Differential Signalling*, TMDS [4]) lub w niektórych trybach pracy drukarek laserowych (rys.3b i c). Obecność w odtwarzanych obrazach tylko krawędzi pionowych lub ukośnych elementów graficznych (słabe cechy dystynktywne, podatne na

[1] Norma TEMPEST (Temporary Emanation and Spurious Transmission) została nadana programowi ochrony przed niekontrolowaną emisją ujawniającą, który powstał w latach 50-tych w USA na zlecenie Pentagonu. Na przestrzeni lat standard ten był wielokrotnie modyfikowany i publikowany pod różnymi nazwami (NAG1A, FS222, NACSIM 5100, NSCD). W roku 1984 stworzona została instrukcja NACSI (National Security Instruction) 5004. Jest ona klasyfikowana jako tajna i określa procedury dla wydziałów oraz przedstawicielstw mające na celu określenie środków bezpieczeństwa wymaganych dla urządzeń przetwarzających dane o znaczeniu dla bezpieczeństwa narodowego Stanów Zjednoczonych.

[2] Font komputerowy jest zbiorem czcionek (znaków: liter, cyfr, symboli specjalnych). Np. *Arial Pogrubiony* to font, a zbiór fontów to krój.

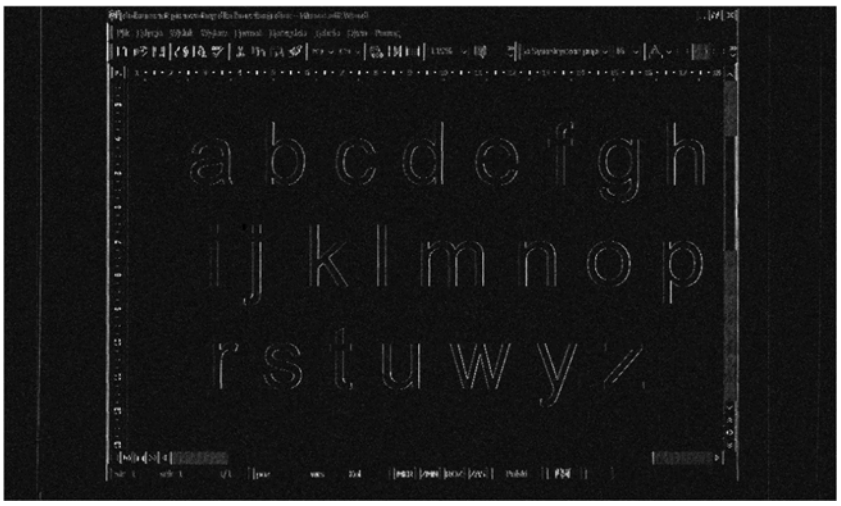
zaburzenia wewnątrzkanałowe) sprawia, że analogowy standard graficzny VGA jest nadal bardzo popularny w niejawnych systemach informatycznych.



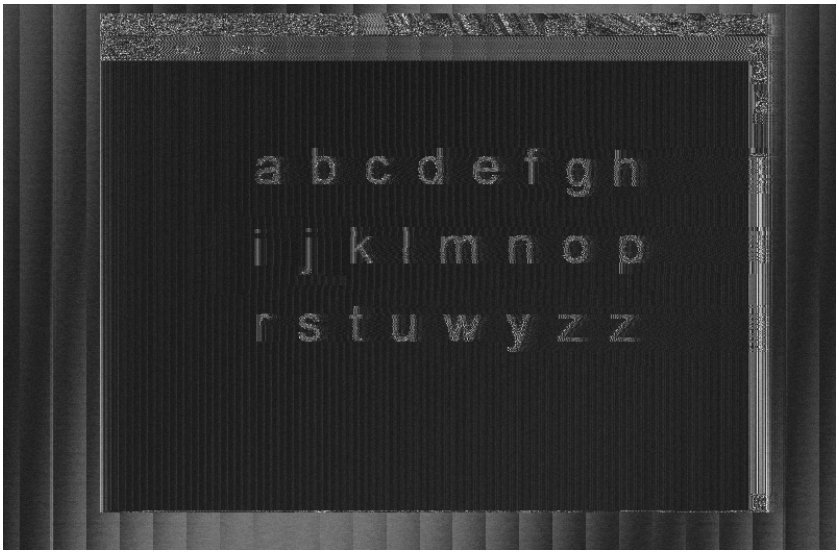
Rys.2. Cechy charakterystyczne fontów tradycyjnych

Należy również zwrócić uwagę na fakt, że w każdym niemal typie urządzeń przetwarzających dane graficzne (np. monitor, drukarka, projektor, skaner), obok interfejsu analogowego występują także interfejsy cyfrowe (DVI/HDMI, DisplayPort), które muszą być obiektem analiz pod kątem bezpieczeństwa EM. Biorąc to pod uwagę, dokonano analizy możliwości bezinwazyjnego pozyskiwania danych od źródeł emisji ujawniających nie tylko w postaci wspomnianego interfejsu analogowego, ale również w postaci interfejsów cyfrowych.

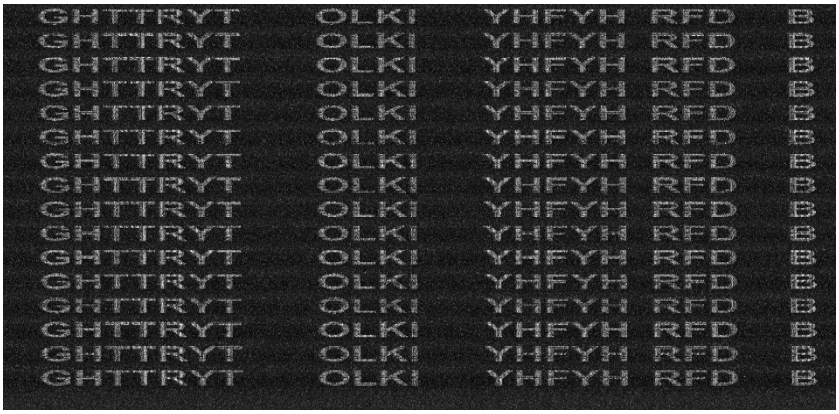
(a)



(b)



(c)



Rys.3. Przykłady odtworzonych obrazów na bazie emisji ujawniających dla: (a) standardu VGA, font Arial (f_o = 614 MHz, BW = 50 MHz), (b) standardu DVI, font Arial (f_o = 824 MHz, BW = 100 MHz), (c) drukarki laserowej, pracującej w trybie Best 600×600 dpi, dwudiodowy układ lasera, font Arial (f_o = 666 MHz, BW = 20 MHz)

Wstępne wyniki badań pokazały, że interfejsy te są źródłem emisji EM o znacznych poziomach, których cechy charakterystyczne są skorelowane z przetwarzanymi danymi. Zatem żaden ze standardów (VGA, DVI/HDMI, DisplayPort) nie może być bezkrytycznie używany w przetwarzaniu danych, zwłaszcza danych wrażliwych.

Omawiane powyżej aspekty wymusiły konieczność szukania nowych, tańszych rozwiązań, które co najmniej w porównywalnym stopniu – jak w przypadku dotychczasowych realizacji architektury urządzeń – będą chronić dane przed infiltracją EM. Ponadto nowe rozwiązania nie powinny naruszać pierwotnej konstrukcji urządzeń komercyjnych stosowanych do budowy urządzeń klasy TEMPEST.

Cyt. z pisma Zarządu VI Służby Kontrwywiadu Wojskowego (załącznik nr 8):

> *Wszelkie prace zmierzające do zwiększenia stopnia ochrony informacji niejawnych poprzez zastąpienie dotychczasowych rozwiązań, w postaci zmian konstrukcyjnych urządzeń lub wspieranie obecnych, są zdaniem SKW akceptowalne i pożądane. Dotyczy to przypadków, kiedy informacje są niejawne i muszą być przetwarzane w sposób umożliwiający ich odczytanie przez człowieka. W takich sytuacjach*

obserwowana informacja np. na monitorze komputerowym lub drukowana musi być czytelna dla człowieka, natomiast towarzyszące tym źródłom emisje, powinny być bezużyteczne w procesie infiltracji elektromagnetycznej.

Oryginalnym podejściem są rozwiązania programowe, których podstawę stanowią specjalnie zaprojektowane fonty komputerowe, jako główne osiągnięcie naukowe habilitanta.

Celem naukowym przedstawionej monografii jest zaprezentowanie nowego podejścia w obszarze rozwiązań zapewniających ochronę EM przetwarzanych danych tekstowych w niejawnych systemach informatycznych. Monografia zawiera:

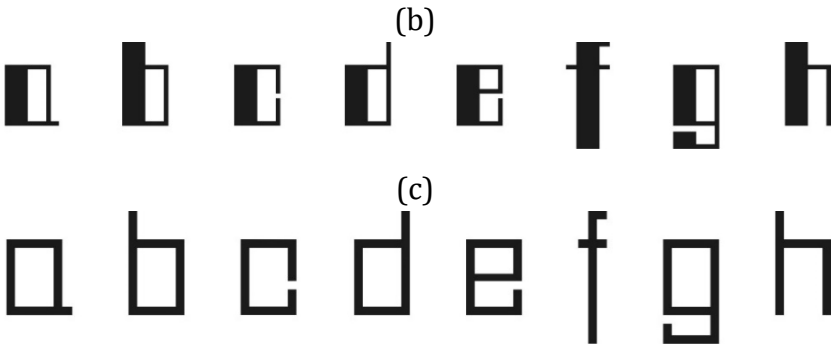
- analizy aktualnego stanu wiedzy i rozwiązań w zakresie metod ochrony informacji przed EM przenikaniem [18, 43];
- podstawowe wymagania dotyczące zasad projektowania i budowy fontów bezpiecznych w kontekście możliwości ich wykorzystania w procesie przeciwdziałania podsłuchowi EM [10];
- analizę korelacyjną znaków małych i wielkich liter oraz cyfr – dla fontów bezpiecznych – na wejściu i wyjściu Kanału Przenikania Informacji (KPI);
- praktyczną weryfikację proponowanego rozwiązania i jego skuteczności w ochronie EM przetwarzanych informacji tekstowych, dla analogowego standardu wideo VGA, cyfrowych standardów wideo DVI/HDMI, DisplayPort oraz dla torów graficznych drukarek laserowych (jedno- i dwudiodowych oraz z listwą diod LED [15]).

W monografii opisano obecny stan ochrony informacji przed EM przenikaniem – zarówno w obszarze technicznym, jak i organizacyjnym oraz prawnym. Przyjęto założenia jakie powinien spełniać font bezpieczny:

- odpowiednia czytelność, wyrazistość i kontrast (brak rozmytych krawędzi);
- wysoki stopień podobieństwa między znakami fontów, zarówno na wejściu, jak i wyjściu KPI;
- niezmienność właściwości graficznych fontów podczas skalowania;
- odporność na proces infiltracji EM (dla źródeł emisji w postaci analogowego i cyfrowego toru graficznego (VGA, DVI/HDMI, DisplayPort) oraz lasera drukarki);
- ograniczenie możliwości odtworzeniowych, wykorzystujących metody cyfrowego przetwarzania obrazów i sygnałów (ujęte m.in. w monografii *Metody analizy i cyfrowego przetwarzania obrazów w procesie infiltracji elektromagnetycznej,* Ireneusz Kubiak, ISBN 978-83-62954-86-5);
- utrudnienie procesu kopiowania dokumentów poprzez OCR (ang. *Optical Character Recognition*);
- ograniczenie wykorzystania znakowej korelacji dwuwymiarowej w procesie cyfrowego przetwarzania obrazów.

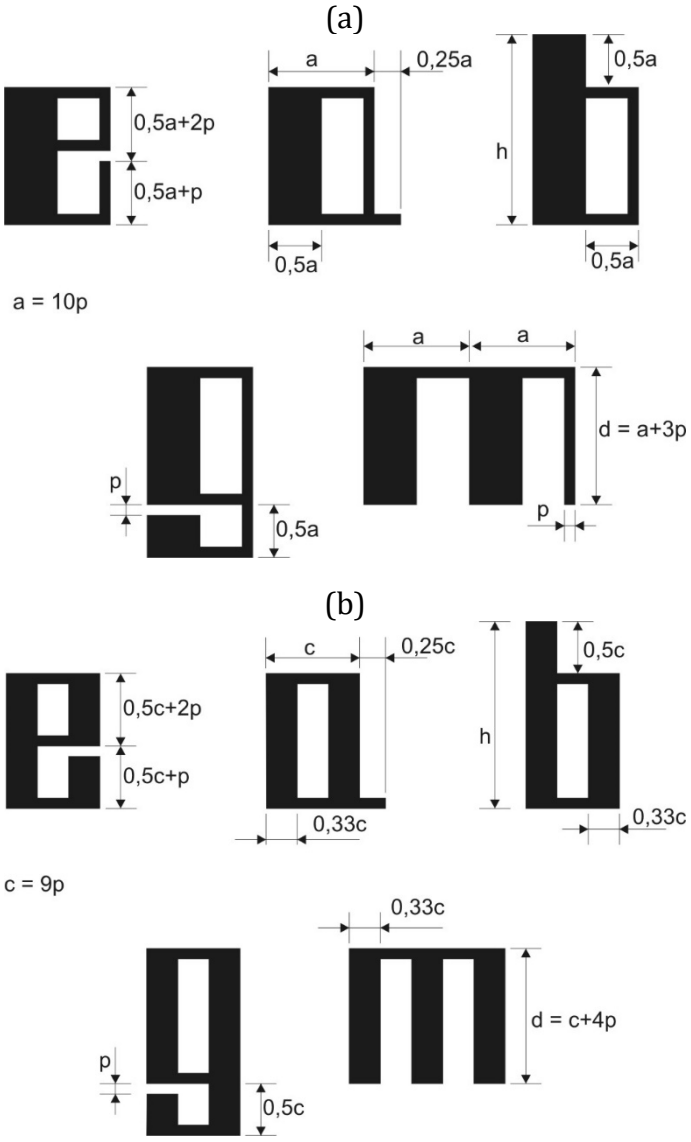
Zaproponowano trzy rodzaje tzw. fontów bezpiecznych, nazwanych odpowiednio jako font: Bezpieczny Symetryczny, Bezpieczny Niesymetryczny i Bezpieczny Prosty (rys.4), z podaniem opisu konstrukcyjnego i proporcji elementów ich budowy (rys.5).

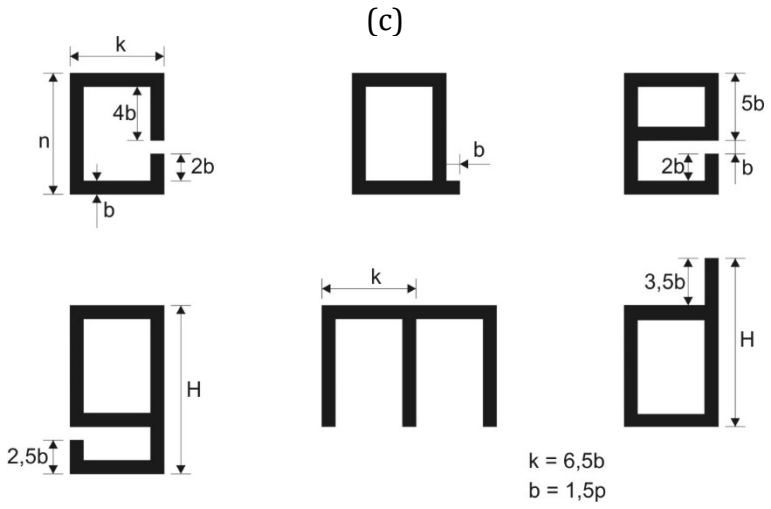
(a)



Rys.4. Postacie przykładowych znaków małych liter fontów bezpiecznych: (a) Bezpieczny Symetryczny, (b) Bezpieczny Niesymetryczny, (c) Bezpieczny Prosty

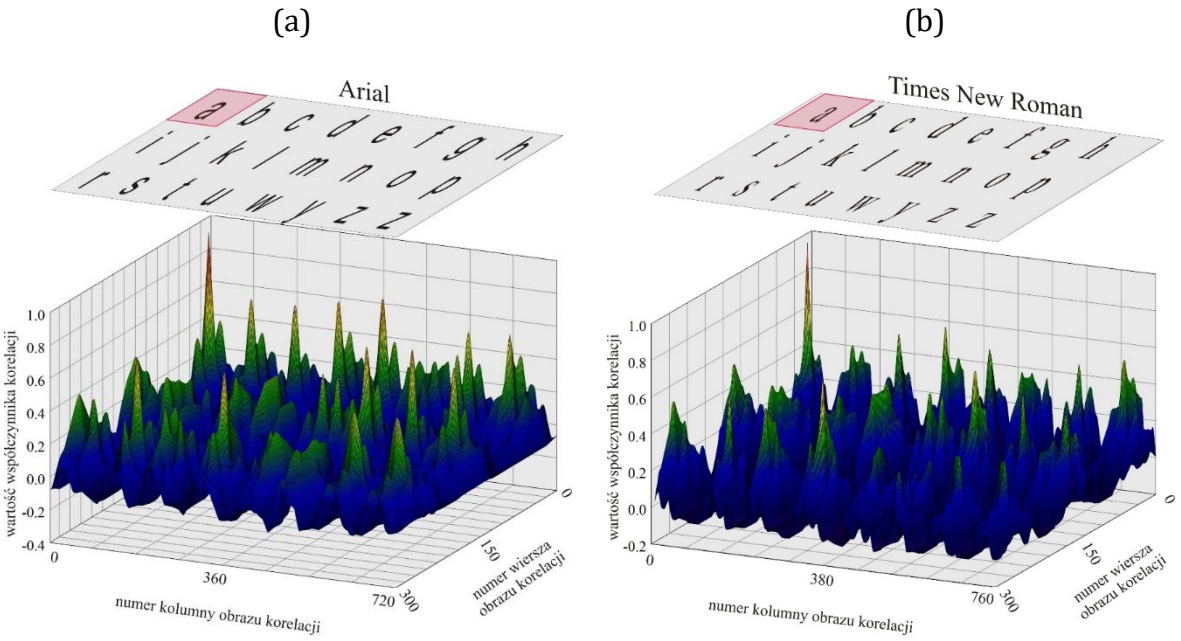
Kształty fontów uwzględniają właściwości KPI typu promieniowanego, który zachowuje się jak filtr górnoprzepustowy. Nazwy fontów bezpośrednio wiążą się z ich kształtami. W pierwszym przypadku znaki liter i cyfr zbudowane są z linii pionowych o jednakowych szerokościach, różniących się od szerokości linii poziomych, a w drugim – szerokości występujących linii pionowych nie są jednakowe.



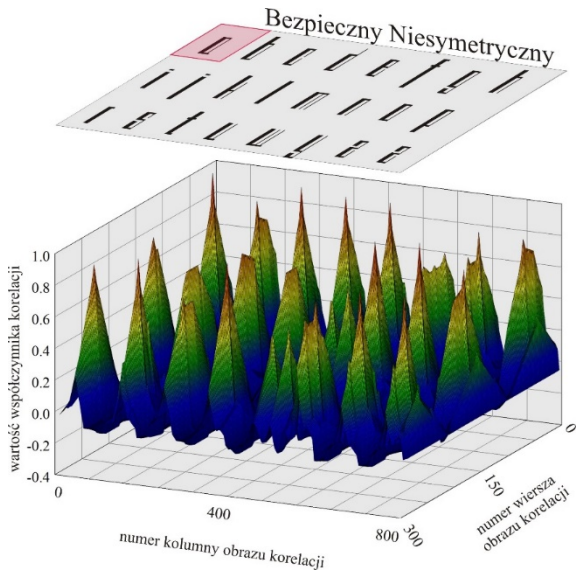


Rys.5. Parametry budowy znaków fontów bezpiecznych: (a) Bezpieczny Niesymetryczny, (b) Bezpieczny Symetryczny, (c) Bezpieczny Prosty

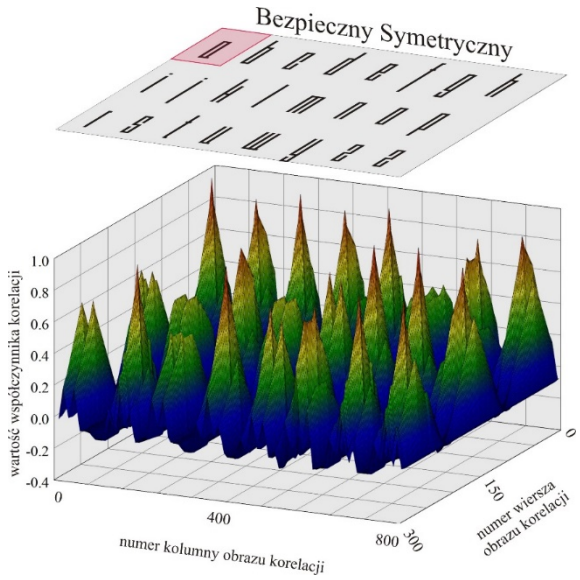
W obydwu przypadkach ma się do czynienia z tzw. krojem pisma dwuelementowego, czyli takiego jak np. Times New Roman. Trzeci typ fontu to litery i cyfry zbudowane z linii pionowych i poziomych o jednakowej szerokości (tzw. krój pisma jednoelementowy, jak np. Arial). Każde z rozwiązań jest skuteczne pod względem odporności na proces infiltracji EM. Fonty bezpieczne nie posiadają cech dystynktywnych przedstawionych na rys.2. W ten sposób uzyskano wysoki stopień podobieństwa (rys.6) między znakami w porównaniu do fontów tradycyjnych oraz fontów, które mogłyby być rozważane jako przydatne w przeciwdziałaniu procesowi infiltracji EM. Fontami, które można rozważać w kategoriach bezpieczeństwa EM, są fonty Sang Muna (Cross, Flower i Noise) oraz font Null Pointer ([9], rys.7), dla których poziom podobieństwa między znakami i rozpoznawalności znaków w procesie infiltracji EM jest znacznie niższy od fontów bezpiecznych.



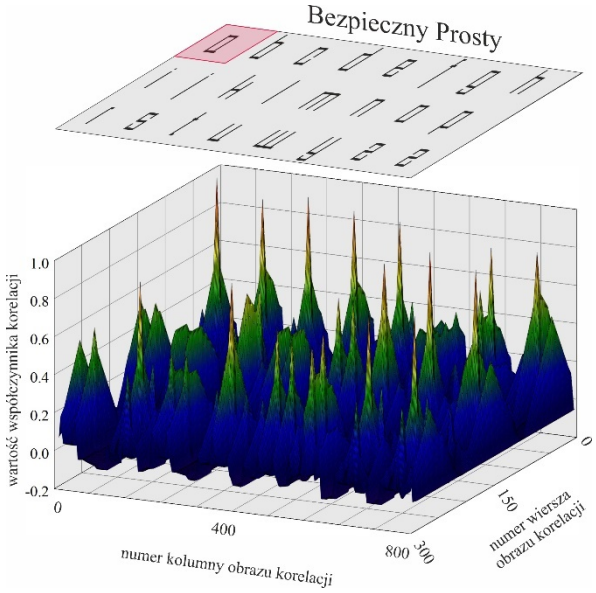
(c)



(d)



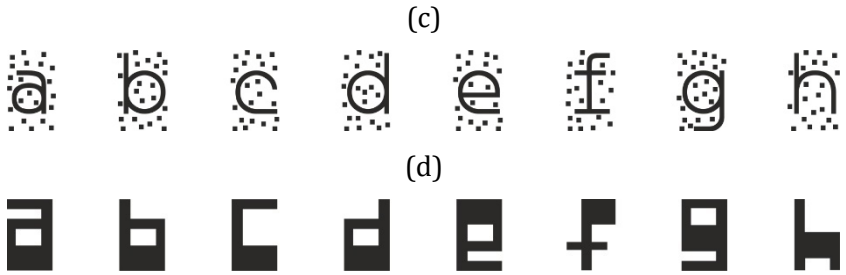
(e)



Rys.6. Przykłady obrazujące stopień podobieństwa między małą literą *a* a pozostałymi literami dla fontów: (a) Arial, (b) Times New Roman, (c) Bezpieczny Niesymetryczny, (d) Bezpieczny Symetryczny, (e) Bezpieczny Prosty, na wejściu KPI

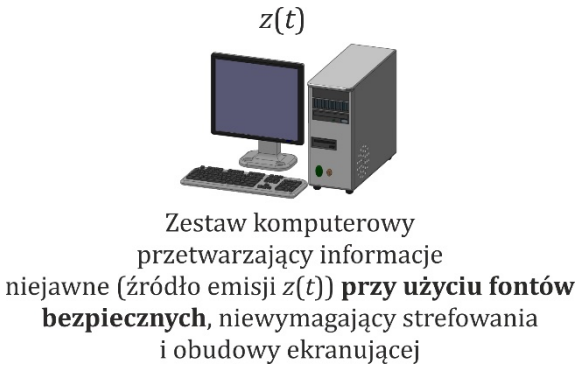
(a)

(b)



Rys.7. Postacie przykładowych znaków małych liter fontów Sang Muna: (a) Cross, (b) Flower, (c) Noise i (d) Null Pointer

Można zatem wysunąć tezę, że fonty bezpieczne są rozwiązaniem, które może zastąpić dotychczas stosowane metody ochrony informacji przed EM przenikaniem – i przedstawić to rozwiązanie w postaci graficznej jak na rys.8.



Rys.8. Sposób ochrony EM informacji przed infiltracją EM bazujący na fontach bezpiecznych (metodę należy rozpatrywać wraz z metodami przedstawionymi na rys.1)

Jak wcześniej wspomniano głównym założeniem projektowym nowych fontów bezpiecznych była maksymalizacja podobieństwa między znakami w ramach danego fontu, przy zachowaniu wymaganego stopnia czytelności fontów. Celem weryfikacji przyjętego założenia, dla każdego fontu przeprowadzono analizę korelacyjną między znakami. Wyznaczono wartości współczynnika korelacji i pogrupowano je zgodnie z przyjętymi przedziałami stopnia podobieństwa (tab.1). Pozwoliło to ocenić istniejące fonty w zakresie możliwości ich stosowania w ochronie przetwarzanych danych tekstowych przed bezinwazyjnym pozyskiwaniem.

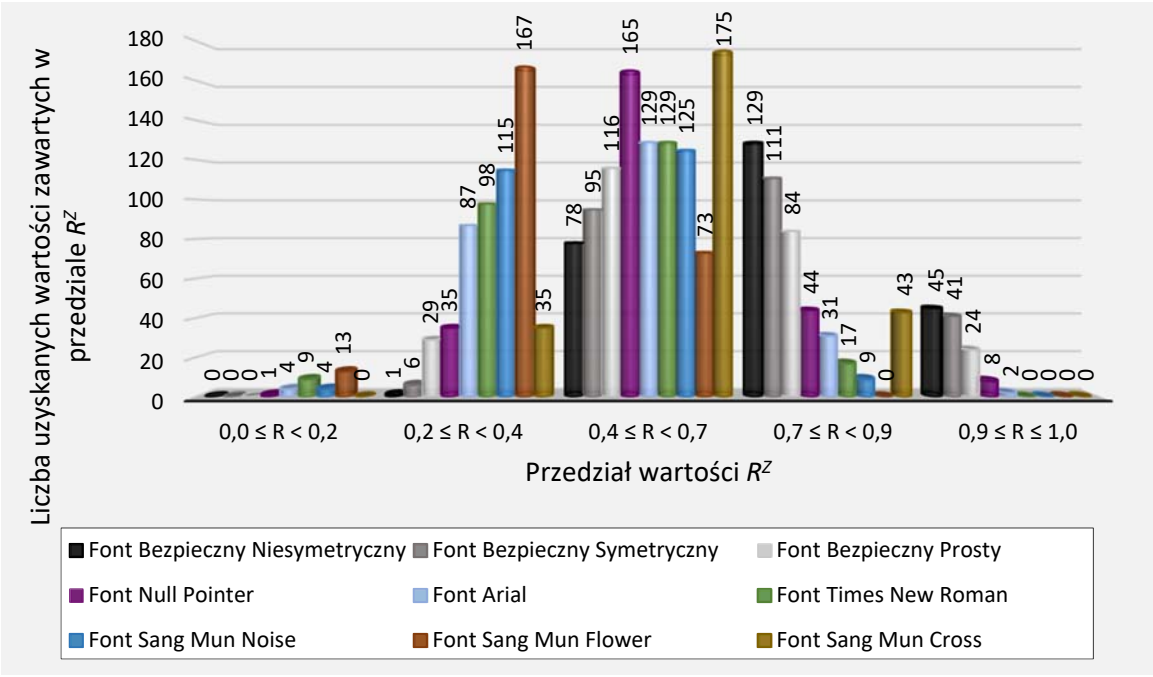
Na rys.9 przedstawiono liczbę uzyskanych wartości współczynnika korelacji znakowej między znakami małych liter, zawartych w zadanych przedziałach. Dla uproszczenia analizy uzyskane wartości współczynnika korelacji (dla fontów: Bezpieczny Symetryczny, Bezpieczny Niesymetryczny, Bezpieczny Prosty, Arial i Times New Roman) porównano z pozostałymi fontami, których szczegółowa analiza została przeprowadzona w [10]. Łatwo można zauważyć, że font Null Pointer, posiadający w swoich kształtach cechy fontu bezpiecznego (font zbudowany tylko z linii pionowych i poziomych), charakteryzuje się dużo mniejszym stopniem podobieństwa międzyznakowego. Pod tym kątem wypada jednak lepiej niż font Arial czy też font Times New Roman.

Tablica 1. Liczba znaków (wartość procentowa w odniesieniu do całkowitej liczby znaków) danego fontu (małe litery), dla którego wartość współczynnika korelacji **na wejściu KPI** zawiera się w danym przedziale wartości R^Z

Wartość współczynnika korelacji R^Z	**Liczba znaków danego fontu, dla których wartość współczynnika korelacji R^Z mieści się w zadanym przedziale**								
	BN	**BS**	**BP**	**Arial**	**TNR**	**Null Pointer**	**Sang Mun Cross**	**Sang Mun Flower**	**Sang Mun Noise**
$0{,}0 \leq R^Z < 0{,}2$ brak związku	0	0	0	4 1,58%	9 3,55%	1 0,39%	0	13 5,14%	89 35,18%
$0{,}2 \leq R^Z < 0{,}4$ słaba zależność	1 0,39%	6 2,37%	29 11,46%	87 34,38%	98 38,74%	35 13,83%	35 13,83%	167 66,01%	129 50,98%
$0{,}4 \leq R^Z < 0{,}7$ umiarkowana zależność	78 30,84%	95 37,55%	116 45,85%	129 50,98%	129 50,98%	165 65,23%	175 69,17%	73 28,85%	35 13,84%
$0{,}7 \leq R^Z < 0{,}9$ dość silna zależność	129 50,98%	111 43,87%	84 33,21%	31 12,25%	17 6,73%	44 17,39%	43 16,99%	0	0
$0{,}9 \leq R^Z \leq 1{,}0$ bardzo silna zależność	45 17,79%	41 16,21%	24 9,48%	2 0,81%	0	8 3,16%	0	0	0

Legenda: TNR – Times New Roman, BS – Bezpieczny Symetryczny, BN – Bezpieczny Niesymetryczny, BP – Bezpieczny Prosty

Liczba wartości współczynnika korelacji R^Z, mówiąca o dość silnym i bardzo silnym stopniu zależności, jest dużo mniejsza dla fontu Null Pointer niż dla fontów bezpiecznych. Pod tym względem font Null Pointer zdecydowanie przewyższa wspomniane fonty dla przedziału wartości R^Z mówiących o tzw. umiarkowanej zależności. Opisane wyżej zjawisko może przekładać się na większy poziom podatności infiltracyjnej fontu Null Pointer w porównaniu z fontami bezpiecznymi.



Rys.9. Porównanie liczby znaków (małe litery) rozpatrywanych fontów, dla których wartość współczynnika korelacji **na wejściu KPI** zawiera się w danym przedziale wartości R^Z

Porównywalnymi właściwościami korelacyjnymi charakteryzuje się font Sang Mun Cross, natomiast gorzej pod tym względem prezentują się dwa pozostałe fonty tego autora: Flower i Noise. Wynika to z faktu występujących dodatkowych elementów, które nie powtarzają się dla każdego znaku. Ich umiejscowienie w oknie znaku jest losowe. Ponadto każdy z rozpatrywanych fontów, w aspekcie potencjalnego rozwiązania służącego ochronie przetwarzanych danych przed infiltracją EM, charakteryzuje się niskim poziomem czytelności. Elementy graficzne mające przeciwdziałać skuteczności optycznego rozpoznawania znaków bardzo mocno zamazują postać graficzną litery lub cyfry. Linie imitujące gałązki kwiatów, punkty przypominające szum czy też krzyżujące się linie, dla znaków o typowych rozmiarach 12 czy 14 punktów wręcz uniemożliwiają wyróżnienie głównego znaku z tła towarzyszącej grafiki.

W pierwszym etapie prac, skuteczność proponowanego przez habilitanta rozwiązania wykazano dla analogowego standardu wideo VGA oraz drukarek laserowych jedno- i dwudiodowych [10-11]. Otrzymano wyniki potwierdzające przyjęte założenia dotyczące bezpieczeństwa EM nowego rozwiązania w postaci fontów bezpiecznych. Zainteresowanie nowym podejściem ochrony danych przed infiltracją EM wskazało konieczność kontynuacji prac nad standardami DVI (HDMI) i DisplayPort oraz drukarkami laserowymi z tzw. listwą diod LED. Habilitant otrzymał w tym względzie stosowne pismo z Zarządu VI Służby Kontrwywiadu Wojskowego (załącznik nr 8), w którym stwierdza się, że:

> *Zdaniem specjalistów Zarządu VI SKW, fonty bezpieczne w obecnej formie stanowią duży krok naprzód, wprowadzający poszukiwania metod przeciwdziałających bezinwazyjnemu pozyskiwaniu informacji w nowy obszar rozwiązań, który może wpłynąć w przyszłości na zmianę koncepcji metod ochrony elektromagnetycznej informacji. [...] Nowy, proponowany obszar zainteresowań to próba innego podejścia do zagadnienia. [...] Wykorzystano tu metodę programową, bazującą na kształtowaniu źródła emisji poprzez zmianę struktury sygnału elektrycznego. Takie podejście zakłada likwidację nie skutków, a przyczyn emisji mogących decydować o powodzeniu procesu infiltracji elektromagnetycznej.*

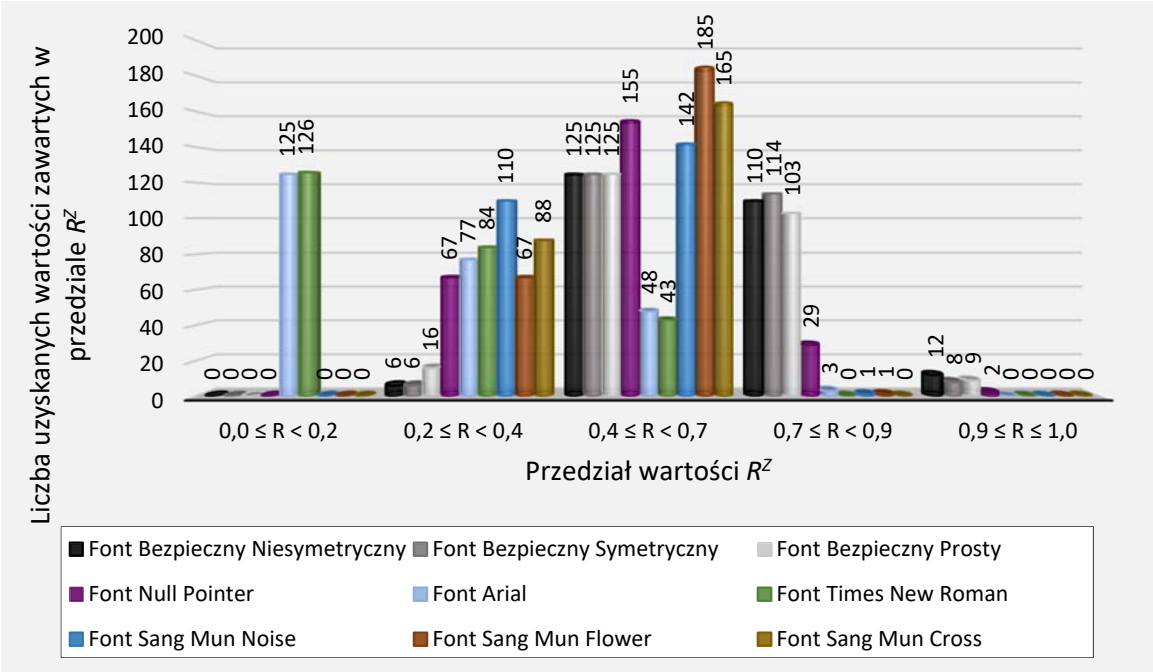
Dalsze prace koncentrowały się zatem nad badaniami i analizą związaną ze skutecznością fontów bezpiecznych w przeciwdziałaniu procesowi infiltracji EM dla toru graficznego wykorzystującego cyfrowy standard wideo DVI.

Wstępne wyniki analiz korelacyjnych fontów Null Pointer oraz Sang Muna na wejściu KPI wykazały, że nie można rozpatrywać tych fontów w kategoriach przydatności w bezpiecznym przetwarzaniu danych tekstowych. Niemniej jednak pełna ocena ww. fontów została dokonana po przeprowadzeniu ich analizy korelacyjnej na wyjściu KPI. Wyniki zamieszczone na rys.10a, b i c pokazują przewagę fontów bezpiecznych nad pozostałymi rozpatrywanymi fontami komputerowymi – w zakresie stopnia podobieństwa między znakami.

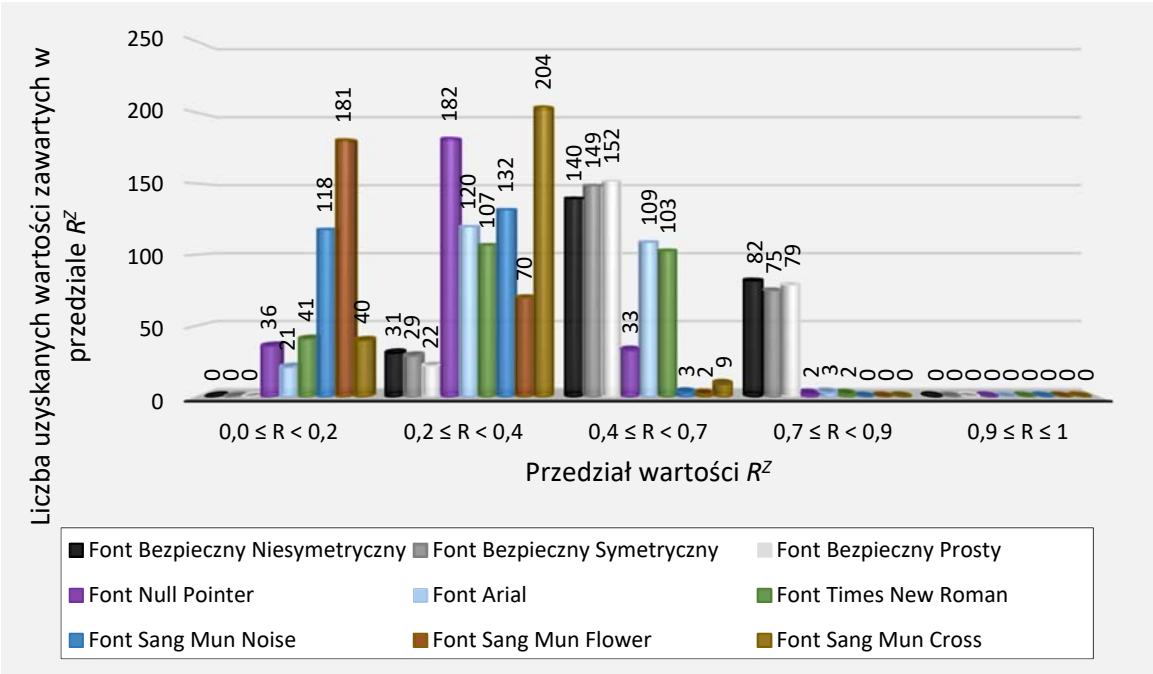
Przydatność fontów bezpiecznych w przetwarzaniu tekstowych informacji niejawnych została potwierdzona uzyskanymi wynikami przeprowadzonych analiz, symulacji komputerowych i badań praktycznych. Podstawę analiz stanowiły metody cyfrowego przetwarzania rzeczywistych sygnałów i odtwarzane na ich bazie obrazy metodą rastrowania, zaimplementowane w Programowym Generatorze Rastra[3] (PGR).

[3] Programowy Generator Rastra (PGR) – aplikacja programowa powstała w trakcie realizacji Projektu Celowego *Sprzętowy i programowy generator rastra jako narzędzie do identyfikacji emisji ujawniających od urządzeń przetwarzających informacje niejawne*. Jest ona akceptowana przez JC SKW lub JC DBTI ABW

(a)

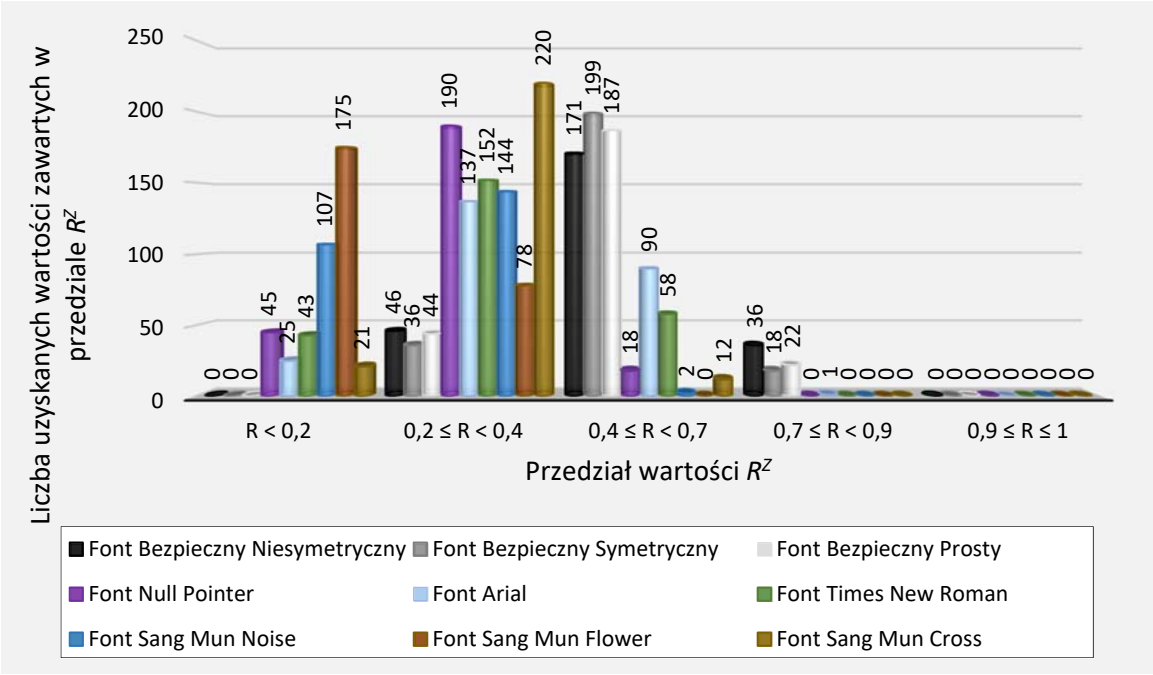


(b)



i wykorzystywana w procesie oceny (certyfikacji) urządzeń przeznaczonych do przetwarzania informacji niejawnych. Aplikacja udostępnia moduły metod (zmodyfikowane na potrzeby procesu infiltracji EM) cyfrowego przetwarzania obrazów i sygnałów umożliwiające: odtworzenie obrazu, sumowanie (uśrednianie) obrazów, progowanie wartości pikseli, rozszerzanie i wyrównywanie histogramów wartości pikseli obrazów, filtrację logiczną filtrami poziomymi i pionowymi, detekcję krawędzi.

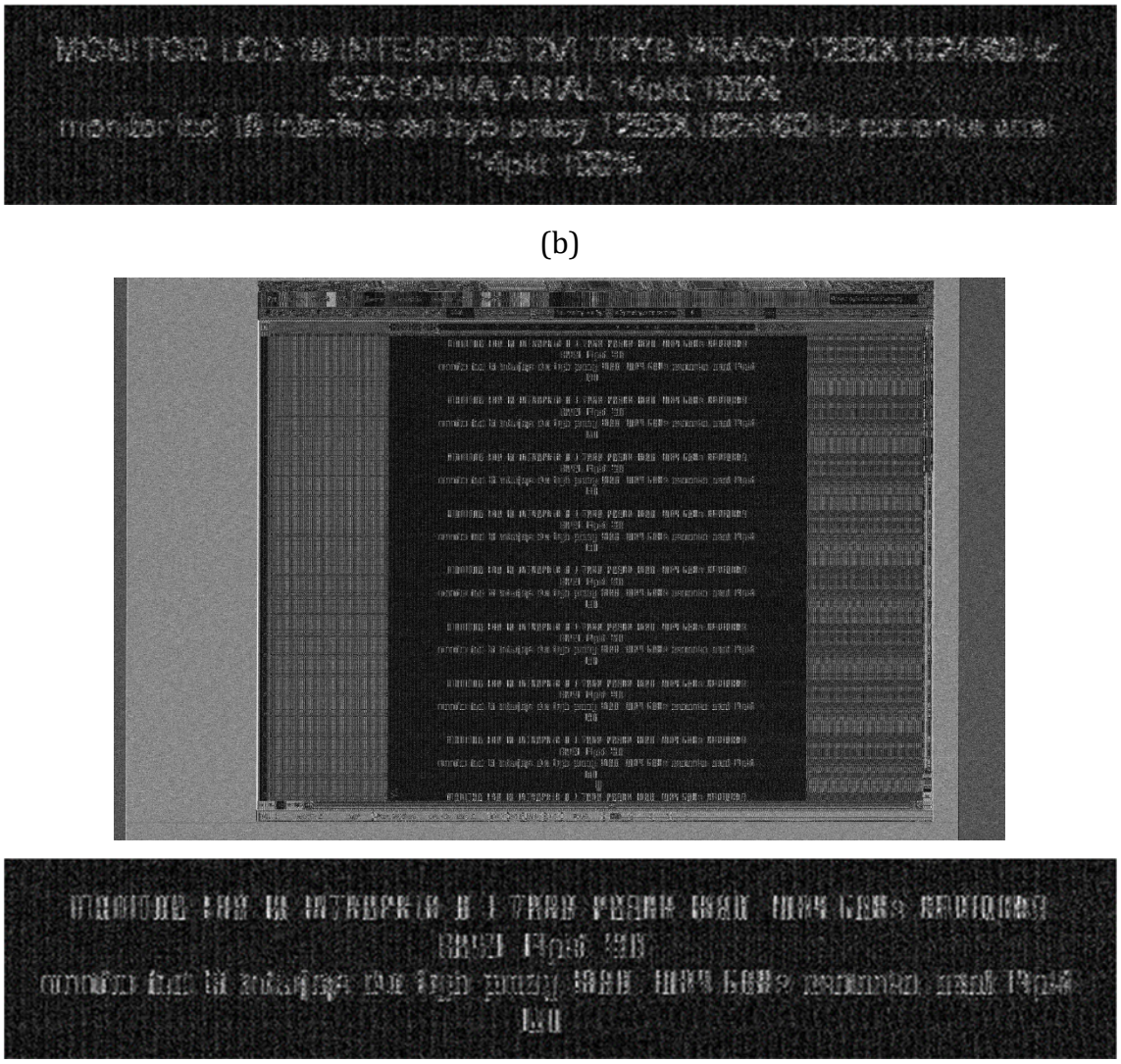
(c)



Rys.10. Porównanie liczby znaków (małe litery) rozpatrywanych fontów, dla których wartość współczynnika korelacji **na wyjściu KPI** zawiera się w danym przedziale wartości R^Z: (a) standard VGA, (b) drukarka laserowa dwudiodowa, (c) standard DVI

W szczególności wykorzystano sumowanie (uśrednianie) obrazów, progowanie wartości pikseli obrazów, filtrację logiczną, a także operacje na histogramach wartości pikseli obrazów. Każda ze stosowanych metod poprawia jakość obrazu, umożliwiając odtworzenie i odczyt danych zapisanych fontami tradycyjnymi (Arial, Times New Roman). Należy podkreślić, że dane zapisane fontami bezpiecznymi, za każdym razem są nieidentyfikowalne.

(a)



(b)

Rys.11. Przykładowe obrazy uzyskane z zarejestrowanych sygnałów emisji ujawniającej, przedstawiające **ciągi znaków liter**, których źródłem jest tor graficzny komputera standardu DVI: (a) font Arial, (b) font Bezpieczny Symetryczny (f_o = 1,73 GHz, BW = 100 MHz, rozmiar znaków 14 punktów)

Wyznaczenie stopnia podobieństwa między znakami fontów bezpiecznych i tradycyjnych było jednym z etapów badań przydatności rozwiązania w ochronie EM przetwarzanych informacji tekstowych. Innym istotnie ważnym zagadnieniem jest podjęcie próby odtworzenia informacji, w oparciu o emisje ujawniające. Analiza wzrokowa, będąca głównym kryterium klasyfikacji odtwarzanych obrazów, w przypadku fontów bezpiecznych staje się mało skuteczna (rys.11), co jest zjawiskiem pozytywnym w aspekcie odporności na infiltrację EM.

Zaproponowano wsparcie analizy wzrokowej analizą decyzyjną wspomaganą komputerowo. W tym celu wykorzystano wartości progowe R^Z_{pr} współczynnika dwuwymiarowej korelacji znakowej R^Z, dla których określono wymaganą liczbę poprawnie odtworzonych znaków na poziomie ufności równym 90%. Dla tak przyjętych parametrów analizy, przeprowadzono stosowne obliczenia wartości Znakowej Stopy Błędów (ZSB, ang. *Character Error Rate* (CER)), zgodnie z zależnością [10-11]:

$$ZSB = \frac{c+k}{f} = \frac{c+(r-e)}{f}, \tag{1}$$

gdzie:

r – liczba poszukiwanych znaków, występujących w analizowanym obrazie,
c – liczba znaków błędnie rozpoznanych,
e – liczba znaków poprawnie rozpoznanych,
k – liczba znaków nierozpoznanych a poszukiwanych ($k = r - e$),
f – liczba wszystkich znaków występujących w obrazie,

dla obrazów zawierających fonty tradycyjne i fonty bezpieczne, w zależności od wartości stosunku sygnału do szumu. Uzyskane wyniki, wykazały wyższą skuteczność fontów bezpiecznych nad tradycyjnymi w ochronie informacji tekstowych. Wartości ZSB obliczone zgodnie z zależnością (1) dla analogowego i cyfrowego standardu wideo oraz drukarki laserowej, jako źródeł emisji ujawniających, przedstawiono w tablicach 2, 3 i 4.

Tablica 2. Wartości Znakowej Stopy Błędów (×10^{-3}) dla znaków fontów bezpiecznych i tradycyjnych w zależności od SNR_G – standard VGA

Znak	Font Bezpieczny Symetryczny			Font Bezpieczny Niesymetryczny			Font Bezpieczny Prosty			Font Arial			Font Times New Roman		
	SNR_G1	SNR_G2	SNR_G3	SNR_G1	SNR_G2	SNR_G3	SNR_G1	SNR_G2	SNR_G3	SNR_G1	SNR_G2	SNR_G3	SNR_G1	SNR_G2	SNR_G3
a	0	1	24	4	10	96	0	0	2	0	0	3	1	2	3
b	0	18	91	3	0	83	5	2	85	3	3	1	5	2	159
c	7	33	15	4	704	824	0	67	294	0	3	3	3	5	48
d	0	4	171	154	724	789	2	0	174	0	4	3	5	2	2
e	0	321	438	151	736	724	0	52	79	3	3	1	5	5	12
f	1	135	261	123	158	201	102	99	79	0	3	2	53	24	5
g	4	223	447	3	19	4	0	3	303	3	1	11	2	3	2
h	3	> 491	820	3	39	96	3	289	400	1	159	268	0	3	5
i	0	39	692	659	250	71	79	173	123	150	151	86	0	29	52
j	1	138	249	98	166	198	99	111	84	0	2	4	42	18	6
k	0	1	76	0	3	37	0	2	45	0	4	3	2	5	45
l	0	147	277	483	150	25	95	76	52	0	1	3	74	14	3
m	0	1	6	0	45	69	0	2	89	3	3	4	5	3	2
n	14	629	817	0	343	527	2	329	635	3	92	112	3	95	109
o	107	> 671	848	4	396	589	18	423	589	3	3	70	2	5	2
p	1	556	720	4	39	89	18	517	552	3	48	68	0	2	3
r	0	387	560	1	474	809	3	70	80	4	4	4	3	20	202
s	0	87	254	3	365	559	0	2	452	4	1	3	5	3	5
t	1	3	0	0	1	10	0	1	5	3	4	34	2	5	2
u	45	> 695	809	0	98	430	2	300	598	3	4	19	0	5	8
w	0	341	567	0	0	4	3	26	394	4	4	0	0	0	3
y	47	535	717	0	6	21	3	53	47	4	4	3	0	2	3
z	0	186	447	0	78	239	5	673	782	3	4	1	2	2	2

Tablica 3. Wartości Znakowej Stopy Błędów (×10^{-3}) dla znaków fontów bezpiecznych i tradycyjnych w zależności od SNR_D – drukarka laserowa

Znak	Font Bezpieczny Symetryczny			Font Bezpieczny Niesymetryczny			Font Bezpieczny Prosty			Font Arial			Font Times New Roman		
	SNR_D1	SNR_D2	SNR_D3	SNR_D1	SNR_D2	SNR_D3	SNR_D1	SNR_D2	SNR_D3	SNR_D1	SNR_D2	SNR_D3	SNR_D1	SNR_D2	SNR_D3
a	2	3	280	3	122	589	2	7	221	0	3	5	2	5	7
b	5	31	127	5	20	115	0	2	182	0	0	0	2	5	14
c	3	19	484	5	98	654	3	102	170	5	0	73	3	5	24
d	2	5	68	3	15	409	2	2	163	5	0	0	5	2	0
e	2	27	433	0	107	715	2	3	314	2	0	7	5	2	14
f	3	3	6	2	132	214	1	21	134	1	3	87	3	2	11
g	0	7	46	0	19	105	2	2	61	2	3	5	5	2	0
h	2	20	92	2	95	221	0	2	131	0	5	3	2	0	34
i	2	2	10	3	80	430	2	0	19	3	5	53	2	12	46
j	3	2	5	5	111	199	2	26	143	0	2	64	2	6	9
k	0	59	284	3	93	211	2	3	34	2	3	5	3	0	5
l	3	2	5	2	149	278	0	20	151	2	2	143	5	2	8
m	3	4	3	4	2	11	2	3	5	1	2	1	3	4	5
n	5	73	426	5	104	443	3	61	430	0	3	49	5	10	87
o	2	14	311	5	301	693	2	136	577	2	0	32	0	2	51
p	0	5	299	0	3	178	0	2	341	2	2	3	3	5	5
r	5	5	3	2	32	615	3	36	370	2	3	34	3	3	27
s	2	3	267	0	75	640	3	20	166	5	2	2	3	3	2
t	0	34	139	0	19	161	5	2	24	0	0	7	3	0	12
u	5	66	387	2	10	438	2	29	316	0	0	5	5	5	14
w	1	13	21	2	8	15	25	41	206	3	2	3	2	1	5
y	2	14	66	2	10	76	5	29	54	3	2	0	3	0	2
z	3	5	358	2	25	418	5	27	267	3	2	5	2	0	5

Tablica 4. Wartości Znakowej Stopy Błędów (×10^{-3}) dla znaków fontów bezpiecznych i tradycyjnych w zależności od SNR_{DVI} – standard DVI

Znak	Font Bezpieczny Symetryczny			Font Bezpieczny Niesymetryczny			Font Bezpieczny Prosty			Font Arial			Font Times New Roman		
	$SNR_{DVI}1$	$SNR_{DVI}2$	$SNR_{DVI}3$	$SNR_{DVI}1$	$SNR_{DVI}2$	$SNR_{DVI}3$	$SNR_{DVI}1$	$SNR_{DVI}2$	$SNR_{DVI}3$	$SNR_{DVI}1$	$SNR_{DVI}2$	$SNR_{DVI}3$	$SNR_{DVI}1$	$SNR_{DVI}2$	$SNR_{DVI}3$
a	95	91	290	21	21	62	4	7	4	1	1	3	3	4	41
b	4	6	3	10	24	48	6	3	56	1	4	4	1	1	4
c	29	97	101	366	509	792	43	41	36	3	3	10	6	11	7
d	6	25	38	27	95	72	36	72	72	3	4	4	4	4	1
e	86	140	345	38	45	188	11	65	125	0	4	28	0	4	18
f	4	13	212	3	4	46	4	1	3	1	7	3	4	4	10
g	1	7	192	24	195	381	3	7	15	0	1	1	4	4	4
h	3	50	143	35	60	101	49	126	421	4	3	22	4	4	6
i	36	42	69	18	15	17	100	153	498	35	46	76	4	14	48
j	1	3	10	4	1	7	7	39	41	3	4	11	3	4	4
k	36	69	77	1	4	24	11	8	62	4	1	3	3	4	3
l	7	31	8	4	8	28	15	76	15	10	39	11	4	4	8
m	4	4	4	4	1	14	4	3	3	1	3	1	1	4	1
n	223	431	367	49	80	146	65	153	216	3	7	55	3	6	79

c.d. Tablicy 4

o	6	60	142	93	236	550	171	351	638	3	36	136	1	7	69
p	135	114	386	4	4	4	107	376	574	1	4	104	3	6	10
r	4	0	3	41	83	81	275	356	541	3	4	4	7	4	11
s	77	156	296	53	70	151	3	15	29	4	1	83	1	1	4
t	49	74	149	105	147	182	86	119	101	4	7	20	3	4	6
u	98	104	363	259	562	550	6	6	27	4	7	28	1	3	8
w	1	11	22	3	6	17	39	45	202	4	3	4	1	1	3
y	18	63	199	15	157	321	13	60	43	3	4	4	0	4	4
z	111	367	477	3	13	27	93	133	203	3	10	7	1	4	6

Uzyskane wartości liczbowe ZSB wskazują na występowanie znacznych błędów związanych z fałszywie podejmowanymi decyzjami w przypadku fontów bezpiecznych. Dla oceny odporności fontów komputerowych na odtworzenie znaków liter z sygnałów emisji ujawniających, zaproponowano wykorzystanie parametru określającego moc korelacji znakowej ${P^Z}_R$, opisywanego zależnością:

$$P_R^Z = \frac{1}{N \cdot M} \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} (R_{nm}^Z)^2, \tag{2}$$

gdzie:

R_{nm}^Z – wartość współczynnika korelacji znakowej między obrazem wzorca a znakiem o współrzędnych (n, m) zawartym w obrazie analizowanym,

M – liczba kolumn znaków obrazu analizowanego,

N – liczba wierszy znaków obrazu analizowanego.

Przyjmując założenie, że wyższa moc korelacji to wzrost bezpieczeństwa EM fontu komputerowego, można zdecydowanie stwierdzić, że fonty bezpieczne są bezpieczne nie tylko z nazwy. Wartości ${P^Z}_R$ dla fontów bezpiecznych są dużo większe niż dla fontów tradycyjnych [10].

W pracy biurowej powszechnym zjawiskiem jest kopiowanie papierowych wersji dokumentów do postaci elektronicznej, umożliwiającej ich przetwarzanie np. w pakiecie aplikacji Microsoft Office. Pozwala to w krótkim czasie uzyskać wersję dokumentu umożliwiającą dokonywanie poprawek lub uzupełnień – czyli prostego przetwarzania, bez konieczności żmudnego przepisywania – w wyniku czego może powstać nowy dokument.

Wydawałoby się, że przekształcenie dokumentu do postaci elektrycznej nie jest zagadnieniem skomplikowanym – wystarczy zeskanowanie dokumentu. Jak się okazuje, nie jest to takie oczywiste, a problem wydaje się być znacznie poważniejszy. Powstały w ten sposób obraz dokumentu jest *bitmapowym* obrazem strony, który nie może być edytowany. Niezbędne jest, aby każdy element obrazu został przekształcony do postaci znakowej. Do tego wykorzystywane jest oprogramowanie OCR.

Zaprojektowane fonty bezpieczne wykazują, obok odporności na proces infiltracji EM, odporność na działanie programów OCR. Skanowanie treści dokumentu pisanego tymi fontami skutkuje otrzymaniem dokumentu o treści niezrozumiałej dla człowieka. Ciąg znaków nie buduje czytelnych wyrazów, a tym samym zdań, które zawierałyby informację przyswajalną przez człowieka. Dowodem na to są przeprowadzone próby przeniesienia dokumentu z wersji papierowej do wersji elektronicznej (rys.12-13). W procesie wykorzystano jeden z najlepszych tego typu programów (w opinii użytkowników) bez przeprowadzania etapu *uczenia* rozpoznawania znaków fontów bezpiecznych.

Ochrona przed elektromagnetycznym przenikaniem informacji to nierozerwalnie połączone ze sobą dwie kwestie. Pierwsza to rozwiązania konstrukcyjne urządzeń których celem jest obniżenie poziomów emisji elektromagnetycznych skorelowanych z przetwarzaną informacją do wartości uniemożliwiających prowadzenie procesu infiltracji elektromagnetycznej. Druga natomiast to doskonalenie metod cyfrowego przetwarzania sygnałów i obrazów zwiększające możliwości identyfikacji i odtwarzania informacji z sygnałów emisji ujawniających o bardzo niskich poziomach.

Ochrona przed elektromagnetycznym przenikaniem informacji to nierozerwalnie połączone ze sobą dwie kwestie. Pierwsza to rozwiązania konstrukcyjne urządzeń których celem jest obniżenie poziomów emisji elektromagnetycznych skorelowanych z przetwarzaną informacją do wartości uniemożliwiających prowadzenie procesu infiltracji elektromagnetycznej. Druga natomiast to doskonalenie metod cyfrowego przetwarzania sygnałów i obrazów zwiększające możliwości identyfikacji i odtwarzania informacji z sygnałów emisji ujawniających o bardzo niskich poziomach.

Rys.12. Tekst podlegający procesowi optycznego rozpoznawania znaków pisany fontem Bezpieczny Symetryczny i Bezpieczny Niesymetryczny

Dohmna pmed elehtromogoetyeeoym preenilmoiem ioformacji to nieraeemmloie potaoeooe he soba dmie buiestie. Pieiiusea ta foeoiiueooio bonstruheyjne uieadeeh btoiyoh celem |est oboieenie peeiemDui emisji elebtramagnetgeeoynh shoreloiimoyoh e pieetumreona mfoimaoja do uiaitosci umemnelioiiDjiieyBh piDiuadeenie proeesii infiltianji elehtramagaetyosriej. Druga natemiast to doskonalenie metod cyfieiuege pieetuioreonia sygnataai i obroeoui euiiebsea(aoe maeliuiasoi ideatyfibac|i i odtuiaieonia informacji e sygnałów emisji ujauioiDjaegch o bordeo oiebieh poeiomoeh.

Belli DHL piEBlj ElEMrEfTE|EEtjEEri|jni prEEtlIIDlIiEIII ¡rfEfiTCE)! tC niErCEEÍIIIEIIriE pEICEEEEE EE EEÈC tilliiE fclUEEtlE. FIEiIiiIEEE ÍE rEELLÍEEEEÍE hEtlEtlLtlEyiE lifEB.ljEEÍl ktÉl|jEtl EEleíTl (EEt bLEÍÉEEÍE PEEÍEITEI11 EII1ÍE(Í EIE^tíE Íl1E|] EEt|JEE E|JEIi EIIEfEIEIIiEE|JEII E piEEtliiEIEEEE ÍrfEírTIEE)|] tE LLEftESEI LraEÍl1EÉIÍIIiÍE|IIEIjEII pfEUIEIjEEEIE ffEEEEL ÍE|iltíEE(Í EIEIItí E ITE j] EEtjjEE EE¡. [IIIßE EEtEÍTfIESt tE ¿EBIiEEEIeEÍE ÍTEtEIj EIjfiEIIIEQE piEEtIIILíEEEiL E|J|EEtEIII í EbíEEEIII EIHiE^EEEjEEE ÍTEÉIiLLEÉEi ÍIjEltjfihEE¡Í (EültiilEÍEEÍIIE ¡EfEÍÍTEEfl E EpgIIEtËIII EIT1IE¡I E¡EIIIEÍE¡(LEIjEtl E tEftíEE EiEhiEtl pEEIEITEEt],

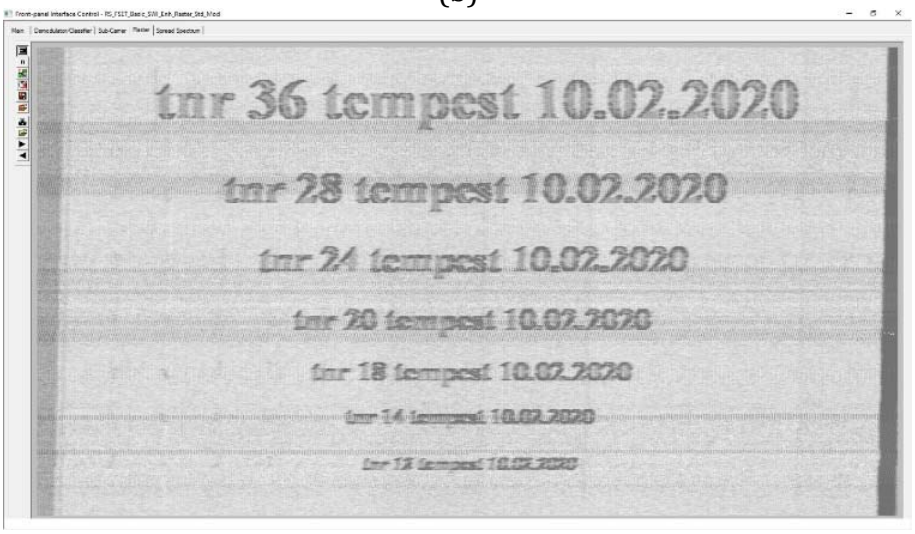
Rys.13. Wynik działania oprogramowania OCR na tekst przedstawiony na rys.12

Osobną część monografii stanowią dodatki, które zawierają zebrane wyniki analiz i badań dla rozpatrywanych źródeł emisji ujawniających, uzupełnione wykresami i obrazami uzyskiwanymi w procesie poprawy jakości odtwarzanych obrazów z wykorzystaniem metod cyfrowego przetwarzania. Duży zasób materiału zgromadzonego w dodatkach pozwala czytelnikowi na samodzielne prześledzenie prowadzonych przez autora rozważań, co nie jest obojętne w poznaniu słuszności przyjętych założeń i wyższości fontów bezpiecznych nad tradycyjnymi, w tak ważnej w obecnych czasach kwestii dotyczącej ochrony informacji niejawnych.

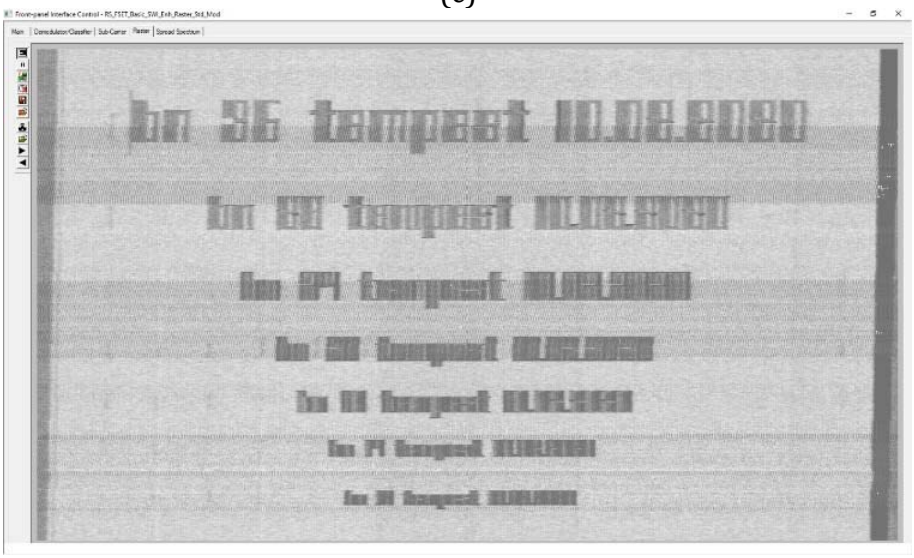
Wstępne badania porównawcze w zakresie możliwości stosowania fontów bezpiecznych zostały przeprowadzone w niezależnym laboratorium Special Telecommunications Services w Bukareszcie. Uzyskane wyniki badań (rys.14), wykonane w oparciu o odbiornik Rohde&Schwarz FSET22 oraz FSWT pokazują, że fonty bezpieczne posiadają cechy, które przeciwdziałają infiltracji elektromagnetycznej. Na podstawie przeprowadzonych wstępnych badań porównawczych i uzyskanych wyników opublikowano artykuł [22].

(a)

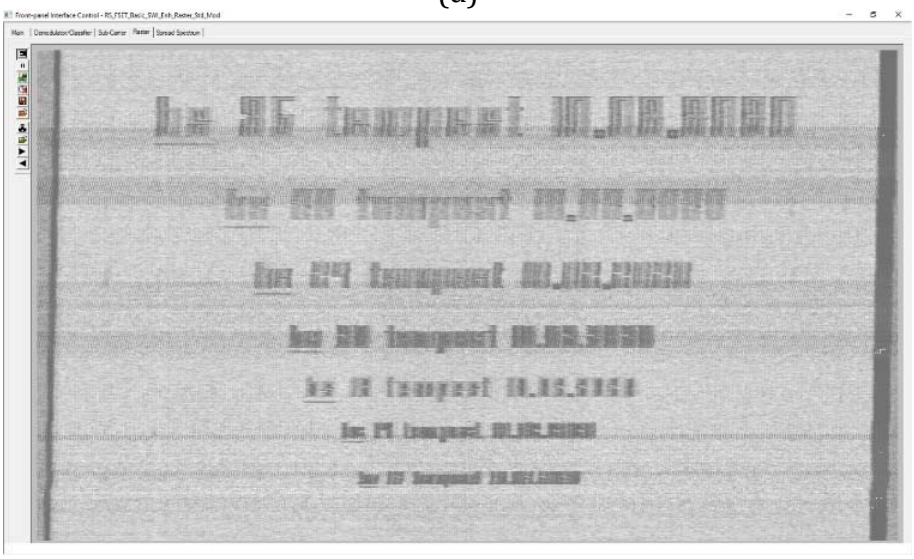
(b)



(c)



(d)



Rys.14. Obrazy zrekonstruowane w oparciu o emisję ujawniającą mierzoną na częstotliwości 910 MHz (*BW* = 10 MHz), przedstawiające: (a) znaki fontu Arial, (b) znaki fontu Times New Roman, (c) znaki fontu Bezpieczny Niesymetryczny, (d) znaki fontu Bezpieczny Symetryczny

Reasumując, można stwierdzić, że do oryginalnego wkładu autora prezentowanej monografii w rozwój metod ochrony informacji przed EM przenikaniem należy:

- analiza wpływu właściwości Kanału Przenikania Informacji na cechy dystynktywne sygnałów, których źródłem jest tor graficzny komputera (standard VGA i DVI/HDMI) oraz laser drukarki, decydujących o postaciach fontów komputerowych uzyskiwanych w odtwarzanych obrazach;
- opracowanie specjalnych kształtów trzech zbiorów fontów bezpiecznych (Bezpieczny Symetryczny, Bezpieczny Niesymetryczny, Bezpieczny Prosty), zapobiegających odtworzeniu informacji metodą rastrowania z rejestrowanych emisji ujawniających, poprzez ich odporność na infiltrację EM, które uzyskały prawo ochronne Urzędu Patentowego RP (patent i wzór przemysłowy);
- odporność fontów bezpiecznych, tworzących dokumentację tekstową, na oddziaływanie programów OCR.

LITERATURA

[1]. Choudary O., Kuhn Markus G., *Template attacks on different devices*, International Workshop on Constructive Side-Channel Analysis and Secure Design, May 2014, pp. 179-198, DOI: 10.1007/978-3-319-10175-0_13.

[2]. Cihan U., Aşık U., Cantürk K., *Analysis of Information Leakages on Laser Printers in the Media of Electromagnetic Radiation and Line Conductions*, International Conference on Information Security and Cryptology; October 2015; Ankara, Turkey.

[3]. Cihan U., Aşık U., Cantürk K., *Analysis and reconstruction of laser printer information leakages in the media of electromagnetic radiation, power, and signal lines*, Computers & Security, 2016; 58: 250-267, DOI: 10.1016/j.cose.2016.02.001.

[4]. Digital Display Working Group, *Digital Visual Interface DVI*, Revision 1.0, 02 April 1999.

[5]. Grzesiak K., Przybysz A., *Emission security of laser printers*, Military Communications and Information Systems Conference, Concepts and Implementations for Innovative Military Communications and Information Technologies, Publisher: House of Military University of Technology, Wroclaw, Poland, 2010, pp. 353–363.

[6]. Kubiak I., *Algorytm wyrównywania histogramu wartości amplitud pikseli obrazu w procesie przetwarzania obrazów uzyskiwanych z sygnałów emisji elektromagnetycznych skorelowanych z sygnałami wideo,* Przegląd Telekomunikacyjny – Wiadomości Telekomunikacyjne, 7/2014, str. 682-686, ISSN 1230-3496.

[7]. Kubiak I., *Cyfrowy (DVI) i analogowy (VGA) standard graficzny w elektromagnetycznej ochronie informacji tekstowych*, Przegląd Telekomunikacyjny – Wiadomości Telekomunikacyjne, 6/2014, ISSN 1230-3496.

[8]. Kubiak I., *Digital processing methods of images and signals in electromagnetic infiltration process*, Image Processing & Communications. Volume 18, Issue 1, Pages 5–14, ISSN (On-line) 1425-140X, DOI: 10.2478/v10248-012-0070-7, April 2014.

[9]. Kubiak I., *Font komputerowy Null Pointer – bezpieczny elektromagnetycznie czy nie?,* Przegląd Telekomunikacyjny – Wiadomości Telekomunikacyjne, 1/2015, ISSN 1230-3496, DOI: 10.15199/59.2015.1.3.

[10]. Kubiak I., *Font komputerowy odporny na infiltrację elektromagnetyczną*, Wydawnictwo Wojskowej Akademii Technicznej, 2014, ISBN 978-83-7938-018-3.

[11]. Kubiak I., *Font komputerowy odporny na infiltrację elektromagnetyczną. Wyniki badań i analiz*, Wydawnictwo Wojskowej Akademii Technicznej, 2014, ISBN 978-83-7938-019-0.

[12]. Kubiak I., *Metody analizy i cyfrowego przetwarzania obrazów w procesie infiltracji elektromagnetycznej*, Wydawnictwo Wojskowej Akademii Technicznej, 2013, ISBN 978-83-62954-86-5.

[13]. Kubiak I., Przybysz A., Musiał S., Grzesiak K., *Generator rastra w procesie infiltracji elektromagnetycznej*, Wydawnictwo Wojskowej Akademii Technicznej, 2012, ISBN 978-83-62954-28-5.

[14]. Kubiak I., *Video signal level (colour intensity) and effectiveness of electromagnetic infiltration*, Bulletin of the Polish Academy of Science – Technical Sciences, Vol.64 No 1, 2016, DOI: 10.1515/bpasts-2016-0023.

[15]. Kubiak I., *LED printers and safe fonts as an effective protection against the formation of unwanted emission,* Turkish Journal of Electrical Engineering & Computer Sciences, Vol. 25, No. 5/2017, DOI: 10.3906/elk-1701-128

[16]. Kubiak I., *TEMPEST font counteracting a non-invasive acquisition of text data,* Turkish Journal of Electrical Engineering & Computer Sciences, Vol. 26, No. 1/2018, DOI: 10.3906/elk-1704-9

[17]. Kubiak I., *The Influence of the Structure of Useful Signal on the Efficacy of Sensitive Emission of Laser Printers,* Measurement, Vol. 1, No. 1/2018, DOI: 10.1016/j.measurement.2018.01.055
[18]. Kubiak I., *Influence of the method of colors on levels of electromagnetic emissions from video standards,* IEEE Transactions on Electromagnetic Compatibility, 28 November 2018, DOI: 10.1109/TEMC.2018.2881304.
[19]. Kubiak I., *Level of Electromagnetic Safety of Graphic Digital Interface*, International Symposium on Electromagnetic Compatibility (EMC EUROPE 2018), 27-30 sierpień 2018, Amsterdam, Holandia, IEEE Xplore 8 październik 2018, DOI: 10.1109/EMCEurope.2018.8484981.
[20]. Kubiak I., Przybysz A., Musiał S., Grzesiak K., *Elektromagnetyczne bezpieczeństwo informacji*, Wydawnictwo Wojskowej Akademii Technicznej, 2009, ISBN 978-83-61486-32-9.
[21]. Kubiak I., Przybysz A., *Drukarki laserowe a skuteczność ataku typu TEMPEST*, Wydawnictwo Wojskowej Akademii Technicznej 2016, ISBN 978-83-7938-117-3.
[22]. Kubiak I., Boitan A., Halunga S., *Assessing the Security of TEMPEST Fonts against electromagnetic eavesdropping by Using Different Specialized Receivers*, Applied Sciences, 2020, 10, 2828, doi:10.3390/app10082828.
[23]. Kuhn Markus G., Ross J. Anderson: *Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations*, in David Aucsmith (Ed.): Information Hiding, Second International Workshop, IH'98, Portland, Oregon, USA, April 15-17, 1998, Proceedings, LNCS 1525, Springer-Verlag, pp. 124-142, ISBN 3-540-65386-4.
[24]. Kuhn Markus G., *Electromagnetic Eavesdropping Risks of Flat-Panel Displays*, 4th Workshop on Privacy Enhancing Technologies, 26-28 May 2004, Toronto, Canada, Proceedings, LNCS 3424, pp. 88–105, Springer-Verlag.
[25]. Kuhn Markus G., *Compromising emanations: eavesdropping risks of* computer *displays*, Technical reports, University of Cambridge, Computer Laboratory, No. 57, December 2003, UCAM-CL-TR-577.
[26]. Lee H.K., Kim J.H., Kim S.C., *Emission Security Limits for Compromising Emanations Using Electromagnetic Emanation Security Channel Analysis*, IEICE Transactions on Communications, 1 October 2013, pp. 2639-2649, https://doi.org/10.1587/transcom.E96.B.2639.
[27]. Litao W., Bin Y., *Analysis and Measurement on the Electromagnetic Compromising Emanations of Computer Keyboards*, Seventh International Conference on Computational Intelligence and Security, 3-4 December 2011, Sanya, pp. 640-643, DOI: 10.1109/CIS.2011.146.
[28]. Loughry J., Umphress DA., *Information Leakage from Optical Emanations*, ACM Transactions on Information Systems Security, 2002; 5: 262–289.
[29]. Loughry J., *("Oops! had the silly thing in reverse")—optical injection attacks in through LED status indicators*, EMC Europe 2019, Barcelona, Spain, 2019.
[30]. Loughry J., Umphress D.A., *Information leakage from optical emanations*, ACM Transactions on Information and System Security 5(3), 2002, 262–289.
[31]. MIL-STD-461F, *Requirements for the control of electromagnetic interference characteristics of subsystems and equipment*.
[32]. Nowosielski L., *Minimalizacja elektromagnetycznej podatności infiltracyjnej urządzeń informatycznych*, 2019, Wydawnictwo Wojskowej Akademii Technicznej, ISBN 978-83-7938-198-2.
[33]. Nowosielski L., Michalak J., *Applications of IT Equipment Protective Solutions against Electromagnetic Compromising Emanations*, 40th Progress in Electromagnetics Research Symposium (PIERS), Japonia 2018.

[34]. Nowosielski L., Przesmycki R., Nowosielski M., *Compromising Emanations from VGA and DVI Interface*, 37th Progress in Electromagnetics Research Symposium, PIERS 2016.
[35]. Nowosielski L., Przesmycki R., *USB 3.0 Interface in the process of Electromagnetic Infiltration*, 37th Progress in Electromagnetics Research Symposium, PIERS 2016.
[36]. Song T.L., Yook J.G., *Study of jamming countermeasure for electromagnetically leaked digital video signals*, IEEE International Symposium on Electromagnetic Compatibility, Gothemburg, Sweden, pp. 1161-1165, 1-4 September 2014, 10.1109/EMCEurope.2014.6931078.
[37]. Telecommunication Standarization Sector of ITU, *Test methods and guide against information leaks through unintentional electromagnetic emissions*, Series K: Protection Against Interference, ITU-T, K.84, 01/2011.
[38]. Tadeusiewicz R., Korohoda P., *Komputerowa analiza i przetwarzanie obrazów*, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1997.
[39]. Tajima K., Ishikawa R., Mori T., Suzuki Y., Takaya K., *A study on risk evaluation of countermeasure technique for preventing electromagnetic information leakage from ITE*, EMC Europe 2017, 4-8 września 2017, Angers, Francja.
[40]. van Eck W., *Electromagnetic radiation from video display units: An eavesdropping risk?*, Computer Security 4(4), 1985, 269–286.
[41]. Nanxuan Z., Ying C., Lau W.H., *Modeling Fonts in Context: Font Prediction on Web Designs*, Computer Graphics Forum, Volume 37, Issue 7, 2018, https://doi.org/10.1111/cgf.13576
[42]. Jun S., Yongacoglu A., Sun D., Dong W., Computer LCD recognition based on the compromising emanations in cyclic frequency domain, IEEE International Symposium on Electromagnetic Compatibility, 25-29 July 2016, Ottawa, Canada, pp.164-169, DOI: 10.1109/ISEMC.2016.7571637
[43]. Lee H.K., Kim J.H., Kim S.C., *Emission Security Limits for Compromising Emanations Using Electromagnetic Emanation Security Channel Analysis*, IEICE Transactions on Communications, 1 October 2013, pp. 2639-2649, https://doi.org/10.1587/transcom.E96.B.2639.
[44]. Tae-Lim S., Yi-Ru J., Jong Y., *Modeling of Leaked Digital Video Signal and Information Recovery Rate as a Function of SNR*, IEEE Transactions on Electromagnetic Compatibility, Vol. 57, 2015, pp. 164-172.
[45]. Nan Z., Yinghua L., Qiang C., Yiying W., *Investigation of Unintentional Video Emanations from a VGA Connector in the Desktop Computers*, IEEE Transactions on Electromagnetic Compatibility, Vol.59, No 6, December 2017, pp. 1826-1834.
[46]. Tokarev A.B., Pitolin V.M., Beletskaya S.Y., Bulgakov A.V., *Detection of informative components of compromising electromagnetic emanations of computer hardware*, International Journal of Computer Technology and Applications, Vol.9, January 2016, pp. 09-19.
[47]. BTPO-500A, *Wytyczne w sprawie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych*.
[48]. SDIP-27/2, *Tempest Requirements and Evaluation Procedures*.
[49]. SDIP-28/1, *NATO Zoning Procedures*.
[50]. Certyfikat ochrony elektromagnetycznej nr 333/2004 wydany przez Departament Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego.
[51]. Ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz.U. 2010 Nr 182 poz. 1228, ze zm.).

5. INFORMACJA O WYKAZYWANIU SIĘ ISTOTNĄ AKTYWNOŚCIĄ NAUKOWĄ ALBO ARTYSTYCZNĄ REALIZOWANĄ W WIĘCEJ NIŻ JEDNEJ UCZELNI, INSTYTUCJI NAUKOWEJ LUB INSTYTUCJI KULTURY, W SZCZEGÓLNOŚCI ZAGRANICZNEJ

5.1. Aktywność naukowa do uzyskania stopnia doktora nauk technicznych

Swoją pracę zawodową rozpocząłem w roku 1992 w Wojskowym Instytucie Łączności na stanowisku inżyniera w pracowni zakłóceń EM zakładu Kompatybilności Elektromagnetycznej (KEM). Realizowane zagadnienia naukowe, tematycznie związane z działalnością pracowni i zakładu, były dla mnie szczególnym wyzwaniem. Od samego początku musiałem poświęcić wiele czasu na przyswojenie specjalistycznej wiedzy w dość rozległej dziedzinie. Jednocześnie uczestniczyłem w pracach badawczych związanych z oceną KEM urządzeń, wprowadzanych na wyposażenie Sił Zbrojnych RP.

Będąc na drugim roku studiów (1988 r.) w Wojskowej Akademii Technicznej, za zgodą Dziekana Wydziału rozpocząłem studia matematyczne na wydziale matematyki, informatyki i mechaniki Uniwersytetu Warszawskiego, które ukończyłem w roku 1993, czyli w drugim roku mojej pracy zawodowej. Po obronie pracy dyplomowej, otrzymałem tytuł magistra matematyki (załącznik nr 7) i objąłem stanowisko starszego inżyniera. W dalszym ciągu prowadziłem badania naukowe i prace rozwojowe związane z analizą emisji promieniowanych i przewodzonych oraz odpornością urządzeń na tego rodzaju emisje. Wyniki prac, które realizowałem samodzielnie bądź zespołowo były zamieszczane w publikacjach naukowych konferencji krajowych i zagranicznych, w których czynnie uczestniczyłem. Brałem udział m.in. w międzynarodowych konferencjach: MKTTA'95 *Teoria i Technika Anten* w Charkowie na Ukrainie (Kubiak I., Aloksa W., *Wybrane wyniki modelowania szerokopasmowego promieniowania anteny dipolowej*), MILCOM'96 IEEE Military Communication Conference w McLean (Kubiak I., *Radiation Characteristics of Antennas Stimulated by a Polychromatic Signal*), MILCOM'97 w Monterey (Kubiak I., *The analysis of distribution of the current in the slender cylindrical antenna*), Regional Conference on Military Communication and Information Systems RCMCIS'99, Zegrze (Kubiak I., Jankowski S., Musiał S., Zając M., Romanik J., *Selected Methods of Limiting of Undesirable Electromagnetic Emission from Electronic Devices*). Do najważniejszych konferencji krajowych w owym czasie zaliczam: Krajowe Sympozjum Telekomunikacji KST'95, Bydgoszcz (Kubiak I., *Analiza promieniowania sygnałów niesinusoidalnych od anten liniowych*), Krajowe Sympozjum Telekomunikacji KST'96, Bydgoszcz (Kubiak I., *Zastosowanie metod momentów do określania natężenia pola od anten liniowych pobudzanych sygnałami niesinusoidalnymi*). Mój artykuł wygłoszony podczas KST w roku 1996 zajął pierwsze miejsce w konkursie na najbardziej interesujący referat zgłoszony przez młodych uczestników.

Rok 1997 był rokiem przełomowym w mojej działalności zawodowej i naukowej. Objąłem stanowisko kierownika pracowni zakłóceń EM i rozpocząłem prace w zakresie tematycznie związanym z ochroną EM przetwarzanych informacji (pkt.II.5,5.1, załącznik nr 2). Bardzo ważnym wydarzeniem dla mnie, jako młodego pracownika naukowego, był udział w realizacji zadań Projektu Badawczego Zamawianego (PBZ) w latach 1996-2000 (nr Z156/T00/96/10). Ważniejsze wykonane przeze mnie prace teoretyczne zamieściłem w załączniku nr 9, a praktyczne w załączniku nr 2 (pkt.II.5,5.2).

Dzięki doświadczeniu jakie zdobyłem w PBZ, swoje zainteresowania skierowałem w stronę zagadnień dotyczących zestawów komputerowych klasy TEMPEST. Urządzenia tego typu stanowią podstawę tworzenia i organizacji systemów niejawnych i autonomicznych stanowisk do przetwarzania informacji wrażliwych. Pojawiło się

zapotrzebowanie na tego typu urządzenia. Były one jednak dostępne tylko i wyłącznie poza granicami naszego kraju (dostępność była ograniczona ze względu na stosowane technologie oraz embarga nakładane przez państwa, w których urządzenia klasy TEMPEST były wytwarzane) i jednocześnie były bardzo drogie. Zostałem zobowiązany do rozpoczęcia prac, których celem miały być krajowe rozwiązania w zakresie modyfikacji komercyjnych zestawów komputerowych na potrzeby przetwarzania informacji niejawnych. Moje działania zaowocowały pozytywną decyzją Komitetu Badań Naukowych (KBN) w sprawie współfinansowania realizacji Projektu Celowego *Wykonanie partii próbnej mikrokomputerów o obniżonym poziomie emisji elektromagnetycznych* (nr 148254/C-T00/99). Projekt zakończył się w 2001 roku po uzyskaniu stopnia doktora nauk technicznych.

Wraz z utworzonym przeze mnie zespołem dokonałem oceny przydatności rozwiązań obniżających poziomy emisji EM (tzw. rozwiązania inżynierii KEM), które następnie zostały z powodzeniem zaadaptowane w urządzeniach w wykonaniu komercyjnym. W efekcie projektu powstał pierwszy krajowy produkt tego typu, spełniający wymagania w zakresie niepożądanych emisji EM (pkt.II.5, 5.3). Jego ogólna dostępność spowodowała znaczne obniżenie kosztów nabycia podobnych rozwiązań pochodzących z zagranicy. Prace w projekcie musiałem pogodzić z pracami związanymi z przewodem doktorskim, który zakończyłem wynikiem pozytywnym 13 grudnia 2000 roku obroną publiczną w Instytucie Telekomunikacji i Akustyki Politechniki Wrocławskiej. Promotorem rozprawy był prof. dr hab. inż. Tadeusz Więckowski. Tytuł rozprawy podany w punkcie 2. autoreferatu nawiązuje do zagadnień ochrony informacji przed EM przenikaniem, które przede wszystkim ukierunkowały mój dalszy rozwój naukowy.

5.2. Aktywność naukowa po uzyskaniu stopnia doktora nauk technicznych

5.2.1. Obszar prac niejawnych

Większość czasu pracy naukowej po uzyskaniu stopnia naukowego doktora nauk technicznych poświęciłem kierowaniu i uczestniczeniu w realizacjach niejawnych prac związanych z ochroną informacji przed elektromagnetycznym przenikaniem. Były to prace wykonywane w ramach niejawnych projektów na rzecz Ministerstwa Obrony Narodowej. W szczególności dotyczyły one:

- opracowywania metod badań emisji ujawniających (zgodnie z zapisami dokumentów BTPO-701A *Wytyczne w sprawie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych,* BTPO-701B *Zalecenia Służby Kontrwywiadu Wojskowego w sprawie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych*, ZOBT-500A *Wytyczne w sprawie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych*, serii dokumentów AMSG, SDIP-27 *Tempest Requirements and Evaluation Procedures* oraz SDIP-28/1 *NATO Zoning Procedures*), które wymagały znajomości najnowszych technologii informatycznych stosowanych w opracowywaniu nowych urządzeń przeznaczonych do przetwarzania informacji niejawnych i stosowanych w Siłach Zbrojnych RP;
- opracowywania metod pozyskiwania sygnałów skorelowanych z przetwarzaną informacją niejawną;

- badań wpływu Kanałów Przenikania Informacji na postać sygnałów emisji ujawniających;
- opracowywania rozwiązań konstrukcyjnych i programowych przeciwdziałających procesowi infiltracji elektromagnetycznej;
- możliwości modyfikacji dostępnych metod cyfrowego przetwarzania sygnałów i obrazów, ułatwiające proces decyzyjny związany z klasyfikacją emisji ujawniających, pochodzących od urządzeń przetwarzających informacje niejawne, przede wszystkim w torach graficznych takich urządzeń.

W ramach tych prac dokonywałem również oceny urządzeń przetwarzających informacje niejawne, wykorzystując wdrożone do użytkowania (przyjęte przez Krajową Władzę Bezpieczeństwa) w Laboratorium WIŁ i opracowane przy moim współudziale Programowy Generator Rastra (zaimplementowane algorytmy cyfrowego przetwarzania sygnałów i obrazów) oraz Sprzętowy Generator Rastra.

Powyższe prace były realizowane na rzecz Bezpieczeństwa i Obronności Państwa nadzorowane przez Służbę Kontrwywiadu Wojskowego oraz Agencję Bezpieczeństwa Wewnętrznego. Ze względu na ich charakter oraz wymagania Ministerstwa Obrony Narodowej co do ich niejawności, wyniki tych prac nie mogły być publikowane, a zatem i cytowane (art. 219 pkt.3 Ustawy Prawo o szkolnictwie wyższym i nauce: *Obowiązek publikacji nie dotyczy osiągnięć, których przedmiot jest objęty ochroną informacji niejawnych*). Niemniej jednak prace, które w pewnym zakresie miały charakter jawny i poznawczy, były i są publikowane w różnych czasopismach naukowych i prezentowane na konferencjach krajowych i międzynarodowych.

5.2.2. Projekty, członkostwo w organizacjach naukowych, współpraca międzynarodowa

Po uzyskaniu stopnia doktora nadal intensywnie realizowałem kolejne przedsięwzięcia naukowe. Współpracowałem i nadal współpracuję z polskimi, jak i zagranicznymi placówkami naukowymi oraz ośrodkami przemysłowymi.

W roku 2002 rozpocząłem pracę w projekcie *Zastosowanie metod inżynierii KEM do zabezpieczenia drukarek komputerowych, monitorów ciekłokrystalicznych oraz komputerów przenośnych przed infiltracją elektromagnetyczną* (nr 148351/C-T00/2002), którym kierowałem. Celem projektu była modyfikacja (zmiany konstrukcyjne jednostki centralnej, modernizacja monitora typu LCD i zastąpienie starego rozwiązania bazującego na monitorze CRT) i dokompletowanie istniejącego zestawu o bezpieczną drukarkę laserową oraz projekt i wdrożenie bezpiecznych rozwiązań dla komputerów przenośnych (pkt.II.5,5.4, załącznik nr 2). Wymagania stawiane w tym obszarze przez Krajową Władzę Bezpieczeństwa były i są bardzo rygorystyczne, a ich spełnienie w zakresie analizy słabych sygnałów i obrazów o niskiej jakości, pozyskiwanych metodami bezinwazyjnymi, wymagało dużego doświadczenia i znajomości zagadnień powstawania źródeł emisji ujawniających i ich rejestracji. W tym czasie powstawało wiele opracowań, które z natury rzeczy były opracowaniami niejawnymi, dotyczących opisów sygnałów emisji ujawniających, metod ich pomiarów oraz odtwarzania informacji. Realizowany projekt zakończył się sukcesem (powstał w pełni funkcjonalny zestaw komputerowy), potwierdzonym wydaniem stosownego certyfikatu ochrony EM na zestaw komputerowy (załącznik nr 10). Do dnia dzisiejszego przyjęte rozwiązania konstrukcyjne mają zastosowanie w produkowanych zestawach komputerowych przeznaczonych do

przetwarzania danych niejawnych; są one wykorzystywane również do organizacji stanowisk w kryptograficznej ochronie informacji.

Wyniki prac obu projektów nie objęte poufnością były publikowane na konferencjach krajowych i zagranicznych oraz w czasopismach naukowych.

Po zakończeniu realizacji projektu celowego, w marcu 2004 roku objąłem stanowisko kierownika Zakładu KEM (które piastuję do dnia dzisiejszego), a w październiku 2007 roku przydzielono mi obowiązki kierownika Laboratorium WIŁ, w ramach którego funkcjonuje Laboratorium KEM i Laboratorium Badań Środowiskowych, a od roku 2016 również Laboratorium Analiz Ataków Cybernetycznych. Różnorodność tematyczna obszarów działalności laboratoriów wymaga ode mnie poświęcenia wiele czasu, również prywatnego, aby można było poznać zagadnienia metod badawczych każdego z laboratoriów.

Dalszy mój rozwój naukowy to uczestnictwo w wielu projektach realizowanych przez WIŁ. Związany on był przede wszystkim z oceną powstających urządzeń ochrony kryptograficznej pod kątem poprawności i skuteczności przyjętych rozwiązań konstrukcyjnych w zakresie ochrony EM. Pozytywne wyniki badań były jednym z wymagań procesu certyfikacji tych urządzeń przez Jednostkę Certyfikującą Służby Kontrwywiadu Wojskowego. W kolejnych latach był realizowany trzeci projekt, w którym pełniłem rolę kierownika prac. Tematem projektu był *Moduł Filtrująco-Kształtujący (MFK) sygnał informacyjny umożliwiający ograniczanie podatności infiltracyjnej urządzeń przeznaczonych do przetwarzania informacji niejawnych* (nr 148448/C-T00/2006), którego efektem były rozwiązania sprzętowe związane z kształtowaniem sygnałów wideo (VGA i DVI) oraz sygnału USB, zmniejszające podatność infiltracyjną urządzeń informatycznych (pkt.II.5,5.5, załącznik nr 2).

Rozwój technologiczny urządzeń przetwarzających informacje niejawne, który nastąpił w ciągu kilku lat, miał istotny wpływ na obniżenie poziomów emisji niepożądanych. Dotyczy to przede wszystkim torów graficznych zobrazowania informacji, którymi są m.in. analogowy standard VGA, cyfrowe standardy DVI, HDMI, DisplayPort czy też układy naświetlania bębnów światłoczułych drukarek laserowych, które są źródłami emisji ujawniających.

Stosowane dotychczas metody oceny źródeł emisji wrażliwych w procesie certyfikacji stawały się niewystarczające. Konieczne było opracowanie i implementacja programowa rozwiązań, które w znacznym stopniu wspomagałyby proces decyzyjny. W szczególności dotyczyło to wspomnianych sygnałów wideo, które były źródłami emisji, i które można obserwować, w postaci odtworzonych obrazów, w czasie rzeczywistym. Dzięki mojej aktywności, przez kolejne lata realizowany był pod moim kierownictwem czwarty już projekt pt. *Sprzętowy i programowy „generator rastra" jako narzędzie do identyfikacji emisji ujawniających od urządzeń przetwarzających informacje niejawne* (nr 148528/C-T00/2009). W ramach tego projektu opracowano algorytmy metod cyfrowego przetwarzania obrazów oraz słabych sygnałów emisji ujawniających i dokonano ich implementacji programowych jako tzw. Programowy Generator Rastra (pkt.II.5,5.6, załącznik nr 2). Jednocześnie ze względu na właściwości sygnałów emisji ujawniających konieczna była modyfikacja wspomnianych algorytmów, które musiały być skuteczne w przypadku bardzo słabych sygnałów emisji wrażliwych. Równocześnie opracowano wersję sprzętową przedmiotowego generatora, będącego źródłem sygnałów synchronizacji pionowej i poziomej mierzonych sygnałów emisji ujawniających dla bardzo szerokiego zakresu pracy kart graficznych komputerów. Umożliwia on odtwarzanie i obserwację w czasie rzeczywistym obrazów przetwarzanych na badanym komputerze. Każde z urządzeń (generatorów) przeszło akceptację stosownych służb,

a wyniki uzyskiwane przy ich wykorzystaniu, stanowią podstawę oceny urządzeń specjalnych przez Jednostki Certyfikujące SKW i DBTI ABW. Zrealizowany projekt umożliwił rozwój aktywności naukowej poprzez odpowiednie publikacje (monografie: *Elektromagnetyczne bezpieczeństwo informacji* (2009, ISBN 978-83-61486-32-9), *Generator rastra w procesie infiltracji elektromagnetycznej* (2012, ISBN 978-83-62954-28-5) i artykuły w czasopismach) w obszarze jawnym.

Wyżej wymienione pozycje książkowe, m.in. mojego autorstwa, stanowiły podstawową lub uzupełniającą literaturę dla przedmiotów wykładanych na wydziale elektroniki Wojskowej Akademii Technicznej w roku 2014/2015:

a) nazwa przedmiotu: *Bezpieczeństwo systemów informacyjnych,* (**Kubiak I.**, Przybysz A., Musiał S., Grzesiak K., *Elektromagnetyczne bezpieczeństwo informacji*);
b) nazwa przedmiotu: *Elektromagnetyczne bezpieczeństwo informacji*, (**Kubiak I.**, Przybysz A., Musiał S., Grzesiak K., *Elektromagnetyczne bezpieczeństwo informacji*, **Kubiak I.**, Przybysz A., Musiał S., Grzesiak K., *Generator rastra w procesie infiltracji elektromagnetycznej*);
c) nazwa przedmiotu: *Podstawy kryptologii*, (**Kubiak I.**, Przybysz A., Musiał S., Grzesiak K., *Elektromagnetyczne bezpieczeństwo informacji*, **Kubiak I.**, Przybysz A., Musiał S., Grzesiak K., *Generator rastra w procesie infiltracji elektromagnetycznej*).

Jedną z najważniejszych publikacji, tematycznie związanej ze wspomnianym projektem, jest monografia mojego autorstwa pt. *Metody analizy i cyfrowego przetwarzania obrazów w procesie infiltracji elektromagnetycznej* (2013, ISBN 978-83-62954-86-5). Praca ma charakter monografii naukowo-technicznej i traktuje o teorii oraz praktyce cyfrowego przetwarzania obrazów uzyskiwanych z sygnałów emisji ujawniających.

Celem naukowym monografii jest przedstawienie nowych metod cyfrowego przetwarzania obrazów i modyfikacja istniejących – wykorzystywanych w typowym przetwarzaniu fotografii cyfrowej. Metody te mają służyć potrzebom klasyfikacji słabych sygnałów, zwanych sygnałami emisji ujawniających, a tym samym i obrazów uzyskiwanych ze wspomnianych sygnałów metodą rastrowania. Konieczność podjęcia prac związanych z nowymi metodami cyfrowego przetwarzania sygnałów i obrazów, służących procesowi infiltracji EM, wynikała wprost z analiz coraz to gorszych jakościowo obrazów odtwarzanych z bardzo słabych sygnałów skorelowanych z sygnałami wideo (tor graficzny systemów teleinformatycznych, laser drukarki laserowej).

Szczególna uwaga została poświęcona czterem zagadnieniom:

- filtracji logicznej filtrem pionowym i poziomym;
- przekształceniom histogramu wartości pikseli budujących analizowany obraz (rozszerzenie wybranego zakresu histogramu, rozszerzenie z wykorzystaniem tablic LUT);
- progowaniu wartości pikseli odtworzonego obrazu;
- metodzie korelacyjnej wspieranej decyzyjnie Filtrem Zerującym.

Opisane w monografii modyfikacje typowych metod cyfrowego przetwarzania obrazów wykorzystywane są w ocenie emisji ujawniających, pochodzących od torów graficznych komputera oraz lasera drukarek komputerowych (urządzeń graficznego zobrazowania danych), ocenianych w procesie certyfikacji nadzorowanym przez Krajową Władzę Bezpieczeństwa. Modyfikacje wspomnianych metod, tj.:

- adaptacja filtracji logicznej filtrem poziomym w odniesieniu do obrazów uzyskiwanych w procesie rastrowania z sygnałów emisji ujawniających,

w których wyraźnie zauważalny jest wpływ właściwości różniczkujących Kanału Przenikania Informacji typu promieniowanego;

- modyfikacja metod cyfrowego przetwarzania obrazów opartych na przekształceniach histogramów wartości pikseli budujących analizowany obraz (rozszerzenie wybranego zakresu histogramu, rozszerzenie z wykorzystaniem tablic *LUT*);
- metoda dwuetapowego progowania wartości amplitud pikseli odtworzonego obrazu, bazująca na wartościach progów, górnego i dolnego, decydujących o minimalizacji wartości amplitud pikseli zakłóceń odtwarzanych obrazów i maksymalizacji wartości amplitud pikseli skorelowanych z poszukiwanymi danymi graficznymi;
- wspomaganie decyzyjne metody korelacyjnej, polegające na wykorzystaniu Filtra Zerującego i kryterium jego działania, dla obrazów silnie zaszumionych, dla których wartości SNR są mniejsze od zera,

znacznie poszerzyły możliwości analiz obrazów i sygnałów skorelowanych z przetwarzanymi, chronionymi informacjami przed EM przenikaniem.

Metody cyfrowego przetwarzania obrazów przedstawione w monografii są aktualnie wykorzystywane w badaniach laboratoryjnych, jako ważny element służący ocenie występujących emisji ujawniających, których źródłem są urządzenia testowane w ramach procesów certyfikacji.

Prowadzone badania naukowe i prace rozwojowe stanowiły ważną bazę merytoryczną dla kierowanego przeze mnie zakładu i laboratorium.

W 2007 roku zostałem przyjęty w poczet członków (ekspertów) Sekcji Kompatybilności Elektromagnetycznej Komitetu Elektroniki i Telekomunikacji PAN, której przewodniczącym jest prof. dr hab. inż. Tadeusz Więckowski. Byłem i jestem członkiem Rady Naukowej Wojskowego Instytutu Łączności .

W mojej działalności można także odnotować prace normalizacyjne, których zakres opisałem w pkt.II.6,6.5 (załącznik nr 2).

Doświadczenie nabyte podczas realizacji prac oraz praktyczne efekty w postaci oprzyrządowania wspomagającego badania urządzeń przeznaczonych do przetwarzania informacji niejawnych, zaowocowały uzyskaniem przez kierowane przeze mnie laboratorium świadectw uznania Jednostki Certyfikującej Służby Kontrwywiadu Wojskowego (nr 6/2011/JC SKW) oraz Jednostki Certyfikującej Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego (nr NZ20450/2012).

Moim doświadczeniem naukowym oraz posiadaną wiedzą staram dzielić się z innymi, m.in. poprzez recenzowanie artykułów oraz udział w zespołach eksperckich NCBiR.

Ostatnie lata mojej aktywności międzynarodowej zaowocowały nawiązaniem współpracy z Profesorem Joe Loughry z Uniwersytetu w Denver w Kolorado. Nasza współpraca dotyczy możliwości pozyskiwania danych metodą bezinwazyjną od różnych rodzajów urządzeń elektronicznych, w szczególności drukarek laserowych. Efektem tego jest wspólna publikacja w czasopiśmie Electronics.

Innym obszarem, w którym podejmujemy wspólne działania są emisje z zakresu częstotliwości widzialnych. Na moje zaproszenie Profesor Joe Loughry napisał rozdział do ostatniej książki, który wprowadza czytelnika w zagadnienia tzw. Optical TEMPEST.
Nawiązałem również współpracę z Profesor Simona Halunga z Politechniki w Bukareszcie (University Politehnica of Bucharest, Electronics, Telecommunications and Information Technology Faculty Bucharest, Romania). Obecnie prowadzimy wspólne badania fontów

specjalnych, których badania prowadzone w niezależnym, zagranicznym laboratorium (Special Telecommunications Services, Bukareszt) potwierdzają właściwości fontów w obszarze przeciwdziałania procesowi infiltracji elektromagnetycznej. Został przygotowany wspólny artykuł do publikacji w czasopiśmie o wysokim współczynniku IF. Podejmujemy również działania w zakresie realizacji wspólnego projektu międzynarodowego.

Moja kariera zawodowa realizowana w ostatnich kilkunastu latach była i nadal jest związana przede wszystkim z tematyką ochrony informacji przed EM przenikaniem. Aspekty niezwykle ważne w przypadkach, kiedy przetwarzana informacja nie może być chroniona kryptograficznie. Wiele wyników prowadzonych prac i wykorzystywanych w codziennej działalności naukowej i badawczej ma charakter niejawny, co w znacznej mierze ma wpływ na ograniczone możliwości publikacji i współpracy z innymi jednostkami naukowymi pracującymi na rzecz instytucji dbających o bezpieczeństwo narodowe.

5.2.3. Uczestnictwo w programach europejskich oraz innych programach międzynarodowych i krajowych

Udział w grupie zadaniowej ds. segmentu naziemnego AGS (ang. Alliance Ground Surveillance) – analiza możliwości integracji naziemnych systemów rozpoznania strategicznego i taktycznego systemu AGS z narodowymi zautomatyzowanymi systemami dowodzenia. Problematyka budowy Sojuszniczego Systemu Obserwacji Obiektów Naziemnych z Powietrza w kontekście wymagań nakładanych na segment naziemny AGS oraz integracji z narodowymi systemami dowodzenia. Określenie zdolności polskich, zautomatyzowanych systemów dowodzenia do współpracy z elementami systemu AGS w zakresie dowodzenia, rozpoznania, analizy, transmisji i zobrazowania danych niejawnych. Wymiernym efektem tego typu przedsięwzięcia ma być zwiększenie tempa operacji, szybkości dowodzenia, stopnia synchronizacji i skuteczności działań na współczesnym polu walki – **udział habilitanta: wykonawca odpowiedzialny za prace realizowane przez WIŁ**.

5.2.4. Udział w konsorcjach i sieciach badawczych

1. Radiostacja przewoźna

Ochrona informacji w sieciach radiowych. Ocena Technicznego Poziomu Zabezpieczenia Urządzeń wchodzących w skład systemu, zgodnie z zapisami dokumentów: BTPO-500A *Zalecenia ogólne SKW w zakresie zapewnienia ochrony elektromagnetycznej systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych* i SDIP-27/2 *NATO Tempest Requirements And Evaluation Procedures*. Analiza parametrów sygnałów radiowych przetwarzanych w systemie z punktu widzenia określenia warunków badań i możliwości identyfikacji sygnałów emisji wrażliwych.

2. Lekki Opancerzony Transporter Rozpoznawczy LOTR

Udział habilitanta związany z obszarem prac obejmujących zagadnienia:

- Analiza rozwiązań konstrukcyjnych LOTR w kontekście wymagań dotyczących instalacji przeznaczonych do przetwarzania informacji niejawnych zgodnie z zaleceniami SKW;
- Określenie wymagań odnośnie poziomów zabezpieczenia urządzeń przeznaczonych do przetwarzania informacji niejawnych znajdujących się w ukompletowaniu LOTR;
- Określenie poziomów zabezpieczenia urządzeń przeznaczonych do przetwarzania informacji niejawnych znajdujących się w ukompletowaniu LOTR (metodyki badań, przeprowadzenie badań, analiza wyników badań w kontekście wymagań SDIP-27/2);
- Rozwiązania konstrukcyjne (modyfikacje) sprzętu umożliwiające osiągniecie wymaganych poziomów zabezpieczenia urządzeń przeznaczonych do przetwarzania informacji niejawnych znajdujących się w ukompletowaniu LOTR.

5.2.5. Kierowanie projektami realizowanymi we współpracy z naukowcami z innych ośrodków polskich i zagranicznych oraz we współpracy z przedsiębiorcami

1. Kompatybilność elektromagnetyczna systemu TETRA Komendy Stołecznej Policji względem innych systemów na terenie Warszawy i okolic. Pomiary praktyczne i analiza dobowej aktywności źródeł emisji celowych i niecelowych w centrum Warszawy oraz w jej okolicach. Przeprowadzono analizę zakłóceń intermodulacyjnych i możliwości instalacji anten nadawczych i odbiorczych w sąsiedztwie istniejących systemów antenowych w lokalizacjach pomiarowych, współpraca z Politechniką Wrocławską – **udział habilitanta: kierownik odpowiedzialny**, lata 2000-2001;
2. Współpraca z Instytutem Technologii Elektronowej (prof. dr hab. inż. Jerzy F. Kołodziejski, dr hab. inż. Jan Łysko) w zakresie skoncentrowanej energii promieniowania EM i sposobów ochrony przed odziaływaniem takiej energii;
3. Współpraca z Uniwersytetem w Denver (Daniel Felix Ritchie School of Engineering and Computer Science, USA, Colorado) w zakresie oceny rozwiązań przeciwdziałających wykorzystaniu emisji EM w pozyskiwaniu informacji klasyfikowanych i możliwości odtwarzania informacji dla źródeł emisji w postaci linii graficznych urządzeń graficznego zobrazowania danych;
4. Nawiązanie współpracy z Politechniką w Bukareszcie (wydział telekomunikacji, profesor Simona Halunga) w zakresie nowych rozwiązań przeciwdziałających infiltracji elektromagnetycznej;
5. Nawiązanie współpracy z instytutem Special Telecommunications Services w Bukareszcie w obszarze przetwarzania sygnałów wideo w zakresie ochrony informacji przed elektromagnetycznym przenikaniem.

5.2.6. Udział w komitetach redakcyjnych czasopism, radach naukowych oraz międzynarodowych i krajowych organizacjach i towarzystwach naukowych

Moje doświadczenie zawodowe w obszarze KEM, ochrony informacji, przetwarzania obrazów i sygnałów (w większości przypadków bardzo *słabych* sygnałów i obrazów o bardzo niskiej jakości) zostało docenione przez środowisko naukowe.

Zostałem zaproszony do współtworzenia wielu czasopism naukowych o wysokiej renomie jako członek rad programowych, zespołu recenzentów czy też redaktor naczelny czasopisma (pkt.II.12, załącznik nr 2). Do najważniejszych elementów w tym obszarze działalności mogę zaliczyć:

- pełnienie z wyboru funkcji redaktora naczelnego w roku 2019 czasopisma *International Journal of Research in Engineering and Innovation* (IJREI) (czasopismo indeksowane w Google Scholar),
- pełnienie funkcji Senior Editor czasopisma *International Journal of Research in Engineering and Innovation* (IJREI),
- na zaproszenie redaktora naczelnego czasopisma *Safety* (Wykaz czasopism naukowych) – pełnienie funkcji redaktora gościnnego (Guest Editor) wydania specjalnego *Electromagnetic Emissions and Its Effects on Human Safety* tegoż czasopisma;
- na zaproszenie redaktora naczelnego czasopisma Applied Sciences (Wykaz czasopism naukowych) – jako redaktor gościnny (Guest Editor) rozpocząłem prace przygotowawcze wydania specjalnego *Confidentiality, integrity, availability and early detection of threats in civilian and military communication systems* czasopisma.

Zostałem również zaproszony do grona zespołu recenzentów wydawnictwa Cambridge Scholar Publishing oraz wydawnictwa IntechOpen. Traktuję te zaproszenia jako wyraz uznania dla mojej wiedzy w obszarach *Computer Security* i przeciwdziałania bezinwazyjnemu pozyskiwaniu informacji.

Od kilku lat, po uzyskaniu stopnia doktora nauk technicznych, jestem członkiem zespołu ekspertów Sekcji Kompatybilności Elektromagnetycznej KEiT PAN. W latach 2000-2002 kierowałem Zespołem Jednostki Certyfikującej Wyroby Wojskowego Instytutu Łączności – Branżowy Zespół ds. Certyfikacji Urządzeń Łączności, Automatyzacji Dowodzenia i Informatyki w zakresie KEM na potrzeby certyfikacji urządzeń wdrażanych do SZ RP. Byłem również członkiem Rady Naukowej Wojskowego Instytutu Łączności w latach 2001-2005 (Sekretarz RN) i 2005-2009 (Z-ca Przewodniczącego RN). Jestem członkiem tej Rady w kadencji 2017-2021 (przewodniczący komisji ds. organizacyjno-finansowych RN).

6. INFORMACJA O OSIĄGNIĘCIACH DYDAKTYCZNYCH, ORGANIZACYJNYCH I POPULARYZUJĄCYCH NAUKĘ

6.1. Osiągnięcia dydaktyczne

Wojskowy Instytut Łączności jest instytucją, która nie posiada w swoim statucie zapisów związanych z prowadzeniem działalności dydaktycznej. Niemniej jednak, ze względu na obszar moich zainteresowań, związanych jednocześnie z kompatybilnością EM i ochroną EM przetwarzanych informacji oraz posiadaną wiedzą w tym obszarze, miałem możliwość występowania w roli wykładowcy i prowadzącego szkolenia. Bardzo istotna jest, jak się niejednokrotnie okazywało podczas wykładów i szkoleń, możliwość połączenia zagadnień KEM z ochroną EM przetwarzanych danych, co spotykało się z dużym zainteresowaniem słuchaczy.

1. Prowadziłem zajęcia w Akademii Obrony Narodowej, Wydział Strategiczno-Obronny, Centrum Symulacji i Komputerowych Gier Wojennych, Zaoczne Podyplomowe Studia Bezpieczeństwa Informacyjnego – Kompatybilność elektromagnetyczna. Zakłócenia promieniowane i przewodzone – 2003 rok;
2. Prowadziłem zajęcia w Akademii Obrony Narodowej, Wydział Strategiczno-Obronny, Centrum Symulacji i Komputerowych Gier Wojennych, Zaoczne Podyplomowe Studia Bezpieczeństwa Informacyjnego – Kompatybilność elektromagnetyczna. Zakłócenia promieniowane i przewodzone – 2004 rok;
3. Prowadziłem zajęcia w Akademii Obrony Narodowej, Wydział Wojsk Lądowych, Niestacjonarne Podyplomowe Studia Bezpieczeństwa Informacyjnego – Kompatybilność elektromagnetyczna urządzeń telekomunikacyjnych w strefie bliskiej, Środowisko elektromagnetyczne i działalność człowieka, Ochrona widma elektromagnetycznego, Modele źródeł zakłóceń – 2005 rok;
4. Prowadziłem zajęcia dydaktyczne z obszaru kompatybilności elektromagnetycznej i ochrony EM przetwarzanych informacji dla studentów wydziału Elektroniki Politechniki Warszawskiej (Instytut Radioelektroniki i Technik Multimedialnych, dr inż. Paweł Kopyt) – 2016 rok;
5. Prowadziłem szkolenie dla pracowników Inspektoratu Uzbrojenia z zakresu stosowania norm obronnych: NO-06-A200:2012 Kompatybilność elektromagnetyczna. Poziomy dopuszczalne *emisji ubocznych i odporności na narażenia elektromagnetyczne*, NO-06-A500:2012 *Kompatybilność elektromagnetyczna. Procedury badań zaburzeń elektromagnetycznych i odporności na narażenia elektromagnetyczne* oraz NO-61-A208:2013 *Zespoły prądotwórcze prądu przemiennego z silnikami spalinowymi. Wymagania ogólne i metody badań* i właściwego definiowania wymagań dotyczących kompatybilności elektromagnetycznej dla nowo pozyskiwanego Sprzętu Wojskowego – 2016 rok.

6.2. Osiągnięcia w zakresie organizacyjnego wsparcia badań naukowych

Organizacyjne wsparcie badań naukowych to m.in. członkostwo w komitetach organizacyjnych tematycznych konferencji naukowych, organizacja sesji specjalnych tych konferencji, jak również pozyskiwanie środków finansowych na zakup aparatury badawczej. W swojej wieloletniej działalności naukowej, a także w trakcie kierowania zakładem KEM i laboratorium Wojskowego Instytutu Łączności, starałem się dbać o rozwój tych komórek organizacyjnych instytutu. Skutkowało to pozyskiwaniem środków finansowych na zakup specjalistycznej aparatury pomiarowej, w wyniku czego możliwe było rozszerzanie zakresu akredytacji Laboratorium WIŁ, zarówno w zakresie KEM jak i ochrony informacji przed EM przenikaniem. Dzięki moim staraniom, w strukturę Laboratorium WIŁ włączono kolejną jednostkę badawczą – Laboratorium Analiz Ataków Cybernetycznych, które uzyskało akredytację Polskiego Centrum Akredytacji. Pozyskałem również środki finansowe na utrzymanie tzw. Specjalnego Urządzenia Badawczego, jakim w przypadku kierowanego przeze mnie Laboratorium jest bezechowa kabina ekranująca wraz ze specjalistycznym oprzyrządowaniem.

W szczególności do moich osiągnięć w zakresie organizacyjnego wsparcia badań mogę zaliczyć:

1. Pełnienie funkcji kierownika Zakładu KEM WIŁ i Laboratorium WIŁ (odpowiednio 2004 – obecnie, 2007 – obecnie); uzyskanie przez Laboratorium Świadectw Uznania

Jednostki Certyfikującej Służby Kontrwywiadu Wojskowego (2010) i Jednostki Certyfikującej Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego (2011), uzyskanie akredytacji Obronności i Bezpieczeństwa (2008) oraz Polskiego Centrum Akredytacji (2013) – umożliwiają realizację badań w pełnym cyklu nadzorowanym przez system jakości zgodnym z PN-EN ISO/IEC 17025 oraz ustawą z dnia 17 listopada 2006 roku *o systemie oceny zgodności wyrobów przeznaczonych na potrzeby obronności i bezpieczeństwa państwa*;

2. Modernizacja infrastruktury laboratoryjnej Instytutu, umożliwiającej prowadzenie badań w zakresie realizacji prac badawczych i rozwojowych w Instytucie, jak i w instytucjach zewnętrznych, poprzez pozyskanie środków na zakup urządzeń:
   - generator CWS500 (EMTEST),
   - oscyloskop cyfrowy DSO 90404 A (AGILENT),
   - system do testów EMC Modula 6000;
3. Przyjęcie w strukturę organizacyjną Laboratorium WIŁ Laboratorium Badań Środowiskowych – 2007;
4. Doposażenie Laboratorium WIŁ w aparaturę do badań odporności urządzeń na oddziaływanie pól EM do częstotliwości 18 GHz (możliwość badań odporności urządzeń na oddziaływanie pól EM o wartościach co najmniej 50 V/m);
5. Przyjęcie Laboratorium Analiz Ataków Cybernetycznych w strukturę organizacyjną Laboratorium WIŁ – 2016 (kierowanie zespołem przygotowującym laboratorium do akredytacji przy Polskim Centrum Akredytacji i Wojskowym Centrum Normalizacji, Jakości i Kodyfikacji);
6. Zakończone sukcesem starania o uzyskanie dofinansowania w zakresie utrzymania Specjalnego Urządzenia Badawczego (SUB – dziesięciometrowa bezechowa kabina ekranująca do badań kompatybilności elektromagnetycznej i ochrony przed EM przenikaniem informacji) na rok 2017 oraz na lata 2018-2020;
7. Uzyskanie w 2017 roku (na okres sześciu lat) przez WIŁ – w oparciu o nadzorowany przeze mnie system jakości Laboratorium WIŁ akredytowany przez Polskie Centrum Akredytacji – upoważnienia do badań technicznych automatów do gier, urządzeń losujących i urządzeń do gier, wydanego przez Ministerstwo Rozwoju i Finansów;
8. Uzyskanie w 2018 roku (listopad) przez podległe mi Laboratorium Analiz Ataków Cybernetycznych akredytacji Polskiego Centrum Akredytacji;
9. Udział w komitetach organizacyjnych konferencji naukowych;
10. Organizacja seminarium międzynarodowego w kierowanym przeze mnie zakładzie dotyczącego tematyki ochrony informacji przed EM przenikaniem.
11. Zgłoszenie na zaproszenie Franka Leferink (International Symposium on EMC, EMC Europe 2018 Conference General Chair) propozycji zorganizowania Sesji Specjalnej podczas konferencji EMC Europe w Amsterdamie (27-30 sierpnia 2018). Tematem sesji były zagadnienia i problematyka związana ze zjawiskiem podsłuchu EM. Tym samym chciałem aby ochrona EM przetwarzanych danych była zaprezentowana szerszemu gronu osób. Temat Sesji Specjalnej: *Electromagnetic eavesdropping (TEMPEST)* został przyjęty i sesja znalazła się w programie konferencji. Zostałem wyznaczony na przewodniczącego sesji.
12. Zgłoszenie na zaproszenie Marco A. Azpúrua (International Symposium on EMC, EMC Europe 2019 Technical Program Chair) propozycji zorganizowania, podobnie jak rok wcześniej, Sesji Specjalnej podczas konferencji EMC Europe w Barcelonie (2-6 września 2019). Tematem sesji były zagadnienia i problematyka związana ze

zjawiskiem podsłuchu EM. Temat Sesji Specjalnej *Electromagnetic eavesdropping (TEMPEST)* został przyjęty i sesja znalazła się w programie konferencji. Zostałem wyznaczony na przewodniczącego sesji.

13. Zgłoszenie na zaproszenie Komitetu Organizacyjnego (International Symposium on EMC, EMC Europe 2020 Technical Program Chair) propozycji zorganizowania, podobnie jak w latach poprzednich, Sesji Specjalnej podczas konferencji EMC Europe w Rzymie (7-11 września 2020). Tematem sesji mają być zagadnienia i problematyka związana ze zjawiskiem podsłuchu EM. Temat Sesji Specjalnej *Electromagnetic eavesdropping (TEMPEST)* został przyjęty.

6.3. Informacja o działalności popularyzującej naukę, udział w zespołach eksperckich i konkursowych, recenzowanie publikacji w czasopismach międzynarodowych i krajowych oraz konferencji międzynarodowych

Praca w instytucie nie ogranicza się tylko do aktywności naukowej poprzez udział w konferencjach, seminariach, czy też poprzez publikacje w renomowanych czasopismach naukowych. Tematyka ochrony informacji w zakresie możliwości jej bezinwazyjnego pozyskiwania stanowi także ciekawostkę popularno-naukową, o czym mogłem się przekonać m.in. podczas *Festiwalu Nauki* (Warszawa 2016). Przedstawiona przeze mnie prezentacja, pokazująca realne zagrożenie utraty informacji poprzez zjawisko EM przeniku informacji, cieszyła się dużym zainteresowaniem.

Zostałem również zaproszony, wraz z moim zespołem, do napisania cyklu artykułów do czasopisma *CSO Magazyn Zarządzających Bezpieczeństwem* oraz *CHIP* (pkt.II.16, załącznik nr 2). W artykułach został przedstawiony problem ochrony informacji przetwarzanych na typowych urządzeniach informatycznych oraz możliwości *wykradania* informacji z tych urządzeń. Istotnie ważnym aspektem było przedstawienie metod technicznych i organizacyjnych, ograniczających podatność infiltracyjną nowych technologii. Wygłosiłem również, na zaproszenie profesora Yevhena Yashchyshyna, trzy seminaria (09.11.2011 r., 13.03.2013 r., 18.12.2013 r.) w Instytucie Radioelektroniki na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej.

Jestem członkiem zespołu eksperckiego Narodowego Centrum Badań i Rozwoju oraz byłem kierownikiem Branżowego Zespołu ds. Certyfikacji Urządzeń Łączności i Informatyki – obszar KEM.

Moim doświadczeniem naukowym oraz posiadaną wiedzą staram się dzielić z innymi – np. poprzez recenzowanie artykułów, wskazując m.in. możliwe kierunki dalszych prac związanych tematycznie ze zgłaszanymi artykułami. Zrecenzowałem ponad 100 artykułów naukowych zgłoszonych do publikacji w międzynarodowych, renomowanych czasopismach i na konferencjach (pkt.II.13, załącznik nr 2).

6.4. Inne osiągnięcia, niewymienione wcześniej

Aktywna działalność w zakresie potwierdzenia kompetencji badawczych podległych laboratoriów (Kompatybilności Elektromagnetycznej i Badań Środowiskowych (BŚ)) przez jednostki zewnętrzne:

- Polskie Centrum Akredytacji;
- Wojskowe Centrum Normalizacji, Jakości i Kodyfikacji;

- Jednostka Certyfikująca Biura Bezpieczeństwa Cybernetycznego Służby Kontrwywiadu Wojskowego (Zarząd VI SKW);
- Jednostka Certyfikująca Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego.

W konsekwencji laboratoria KEM i BŚ, wchodzące w skład kierowanego przeze mnie Laboratorium WIŁ, otrzymały akredytację PCA (AB149) i WCNJiK (1/MON/2010, 11/MON/2011, 17/MON/2014, 17/MON/2017). Laboratorium KEM uzyskało uznania JC BBC SKW i JC DBT ABW potwierdzone zawarciem stosownych umów nr NZ20450/2012 z dnia 09.10.2012 r. (ABW), UL/01/2015 z dnia 16.02.2015 r. (SKW) i wydaniem świadectwa uznania nr 1/2015/JC SKW (wyznaczanie Technicznego Poziomu Zabezpieczenia Urządzenia – TPZU), co pozwala na prowadzenie badań ochrony EM urządzeń przeznaczonych do przetwarzania informacji niejawnych, zgodnie z dokumentami:

- SDIP-27 *NATO Tempest Requirements And Evaluation Procedures*,
- BTPO-701B *Zalecenia Służby Kontrwywiadu Wojskowego w sprawie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych*,

a następnie zgodnie z dokumentami:

- SDIP-27/1 *NATO Tempest Requirements and Evaluation Procedures*,
- ZOBT-500A *Zalecenia ogólne SKW w zakresie zapewnienia ochrony elektromagnetycznej systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych* (zastępuje BTPO-701B),
- SDIP-27/2 *NATO Tempest Requirements and Evaluation Procedures*,
- SDIP-28/1 *NATO ZONING Procedures* – określanie klasy urządzenia przeznaczonego do przetwarzania informacji niejawnych (jedyne laboratorium w Polsce uznawane w tym zakresie przez SKW).

Laboratorium KEM Wojskowego Instytutu Łączności, które wchodzi w skład Laboratorium WIŁ, jest jedynym laboratorium w Polsce posiadającym uznanie Służby Kontrwywiadu Wojskowego (i jedno z nielicznych uznawanych przez Agencję Bezpieczeństwa Wewnętrznego) jako kompetentne do prowadzenia badań ochrony EM urządzeń specjalnych (zgodnie z dokumentem SDIP-27/2) oraz urządzeń komercyjnych (zgodnie z dokumentami ZOBT-500A i SDIP-28/1). Potwierdza to wysokie kompetencje personelu laboratorium prowadzonego pod moim kierownictwem.

7. PODSUMOWANIE DOROBKU NAUKOWO-BADAWCZEGO ORAZ POZOSTAŁYCH OSIĄGNIĘĆ (po uzyskaniu stopnia doktora nauk technicznych)

Moja kariera zawodowa, która rozpoczęła się w roku 1992, od samego początku związana była z zagadnieniami kompatybilności elektromagnetycznej. Z upływem lat, w związku z objęciem stanowiska kierownika pracowni a następnie kierownika zakładu, podjąłem się realizacji zadań związanych tematycznie z ochroną elektromagnetyczną przetwarzanych informacji. Ten obszar tematyczny do dzisiaj jest podstawą mojego rozwoju naukowego.

Po uzyskaniu stopnia doktora nauk technicznych byłem kierownikiem kilku projektów badawczych, których wyniki są wykorzystywane w pracach wdrożeniowych (pierwszy polski komputer klasy TEMPEST, drukarka laserowa i monitor komputerowy klasy TEMPEST) oraz w pracach badawczych (Sprzętowy i Programowy Generator Rastra, Moduł Filtrująco-Kształtujący) realizowanych przez laboratorium Wojskowego

Instytutu Łączności, którego jestem kierownikiem. Zdobyte doświadczenie pozwoliło na uzyskanie przez laboratorium KEM WIŁ (jedno z laboratoriów wchodzące w skład laboratorium WIŁ) świadectwa uznania SKW i ABW oraz akredytacji PCA i WCNJiK. Byłem i jestem wykonawcą wielu innych projektów niejawnych realizowanych przez WIŁ.

W większości realizowane przeze mnie prace są pracami niejawnymi. Jednak w każdej pracy istnieje pewien czynnik poznawczy, który pozwolił mi w ograniczonym zakresie na działalność publikacyjną oraz aktywność na arenie międzynarodowej. Nawiązałem współpracę z Uniwersytetem w Denver (USA) oraz z Uniwersytetem w Bukareszcie w zakresie badań źródeł emisji klasyfikowanych – jako wartościowe w procesie infiltracji elektromagnetycznej. Wyniki prac w obszarze jawnym publikowałem w recenzowanych czasopismach (lista A MNiSW oraz wykaz czasopism naukowych), wygłaszałem podczas konferencji krajowych i zagranicznych (indeksowanych w WoS). Jestem autorem lub współautorem kilku monografii, rozdziału w monografii, patentu oraz wzoru przemysłowego. Jestem twórcą trzech zbiorów fontów bezpiecznych (główne osiągnięcie naukowe w postępowaniu habilitacyjnym), których wykorzystanie zapewnia ochronę przetwarzanych informacji przed elektromagnetycznym przenikaniem. Obecnie prowadzone analizy rozwiązań programowych zmierzają do powszechnego wykorzystania (wdrożenia) fontów bezpiecznych w przetwarzaniu informacji. Współtworzyłem Sprzętowy i Programowy Generator Rastra – urządzenia wspomagające proces certyfikacyjny systemów i urządzeń przeznaczonych do przetwarzania informacji niejawnych. Opiniowałem kilkadziesiąt dokumentów normalizacyjnych, jestem autorem i współautorem kilku norm obronnych. Na zaproszenie komitetów organizacyjnych konferencji międzynarodowych (indeksowanych w WoS oraz Scopus) oraz redaktorów czasopism naukowych (z listy A oraz wykazu czasopism naukowych MNiSW) przeprowadziłem kilkadziesiąt recenzji artykułów. Dwukrotnie prowadziłem sesje specjalne podczas konferencji EMC Europe. Obecnie prowadzę wydanie specjalne czasopisma *Safety* jako Edytor Zaproszony. Byłem członkiem komitetów organizacyjnych kilkunastu konferencji międzynarodowych.

Szczegółowe dane naukometryczne zawiera pkt.IV, załącznik nr 2.

Moja aktywność naukowa i badawcza została doceniona przez moich przełożonych, jak również wydawnictwa naukowe i osoby aktywne naukowo w obszarze KEM oraz w bardzo wąskim obszarze związanym z ochroną informacji przetwarzanych w informatycznych systemach niejawnych. Za całokształt działalności zawodowej zostałem wyróżniony odznaczeniami resorowymi MON. Otrzymałem również nagrody Dyrektora Wojskowego Instytutu Łączności w konkursach *Nauka WIŁ* (pkt.II.17, załącznik nr 2).

Na arenie międzynarodowej, moja specjalistyczna wiedza znalazła uznanie wśród wydawnictw naukowych Cambridge Scholar Publishing (załącznik nr 13) i IntechOpen (załącznik nr 14), do których zostałem zaproszony jako recenzent wydawniczy oraz jako autor rozdziału do wydawnictwa naukowego pt. *Digital distribution*. Profesor Joe Loughry, przed nawiązaniem ściślejszej współpracy, wystosował do dyrektora Wojskowego Instytutu Łączności list rekomendacyjny (załącznik nr 15). Nawiązałem również współpracę z Politechniką w Bukareszcie oraz Special Telecommunications Services w Bukareszcie co pozwoliło mi na zintensyfikowanie prac badawczych w obszarze rozwiązań przeciwdziałających infiltracji elektromagnetycznej.

Ireneusz Kubiak

dr inż. Ireneusz Kubiak