Ireneusz KUBIAK, Artur PRZYBYSZ

Wojskowy Instytut Łączności

doi:10.15199/48.2015.11.12

Wpływ konstrukcji urządzeń komercyjnych na ochronę elektromagnetyczną przetwarzanych informacji

Streszczenie. *Zagrożenie związane z możliwością bezinwazyjnego pozyskiwania informacji poprzez wykorzystanie emisji elektromagnetycznych w obecnych czasach jest bardzo realne. Dla zminimalizowania występowania zjawiska stosuje się szereg przedsięwzięć technicznych, często jednak wpływających negatywnie na wygląd takich urządzeń oraz koszt ich nabycia. Ciągle poszukuje się nowych i tańszych rozwiązań. Często sugeruje się, że rozwiązania takie są gotowe i dostępne na rynku. Przykładem może być drukarka komputerowa wykorzystująca technologię druku opartą na listwie diod LED.*

Abstract. *Nowadays the risk associated with the possibility of non-invasive obtaining information through the use of electromagnetic emissions is very real. In order to reduce the effect of the phenomenon are used the technical solutions which have however an effect on the appearance of modified devices and their purchase costs. All the time engineers look for new and cheaper solutions. Frequently, it is suggested that such solutions are ready and available on the market. An example would be a printer using a technology based on a slat of LEDs (**The impact of commercial equipment designs to electromagnetic protection of data process**).*

Słowa kluczowe: ochrona informacji, emisja elektromagnetyczna, elektromagnetyczne przenikanie informacji, dane graficzne
Keywords: protection of information, electromagnetic emission, electromagnetic leackage information, graphic data

Wstęp

W obecnych czasach, w których powszechne jest przetwarzanie informacji z wykorzystaniem urządzeń elektronicznych szczególnego znaczenia nabiera kwestia bezpieczeństwa tychże informacji. Łatwość przetwarzania skutkuje bowiem łatwością utraty poufności. Informacje mogą być w niekontrolowany sposób przejęte przez osoby trzecie. Jedną z przyczyn takiego stanu rzeczy są emisje elektromagnetyczne, które powstają podczas przetwarzania danych, występujących w postaci sygnałów elektrycznych. Emisje te pozwalają na odtworzenie przetwarzanych informacji [1, 2, 5, 8]. Niezwykle ciekawym a zarazem i niebezpiecznym zjawiskiem jest możliwość odtwarzania danych występujących w postaci graficznej, które w prosty sposób stają się czytelne i zrozumiałe dla człowieka. Do nich możemy zaliczyć dane wyświetlane na monitorze komputerowym czy też drukowane na drukarkach komputerowych. Celem eliminacji źródeł takich emisji, zwanych emisjami ujawniającymi, stosuje się szereg przedsięwzięć organizacyjnych i technicznych, których zadaniem jest obniżenie poziomów wspomnianych emisji elektromagnetycznych w miejscach ich pomiaru, czyli w miejscach dostępnych dla potencjalnych szpiegów. Często stosowanymi przedsięwzięciami technicznymi są metody inżynierii kompatybilności elektromagnetycznej, do których możemy zaliczyć uziemianie, ekranowanie, filtrację obwodów sygnałowych i obwodów zasilania, symetryzację przewodów. Inną, rozwijającą się metodą przeciwdziałającą procesowi infiltracji elektromagnetycznej dla przetwarzanych danych w postaci tekstowej są rozwiązania programowe [3, 4, 5, 6]. Polegają one na wykorzystaniu tzw. fontów bezpiecznych o specjalnych kształtach, które wpływając na postać przebiegów czasowych elektrycznych sygnałów wideo eliminują do minimum występowanie cech dystynktywnych sygnałów emisji ujawniających, umożliwiających odtworzenie informacji.

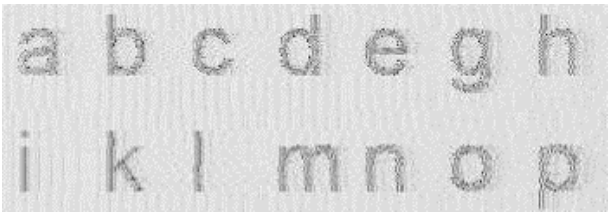
Czasami, w przypadkach specjalnych zestawów komputerowych, określanych mianem zestawów klasy „TEMPEST", pojawiają się sugestie o możliwościach stosowania rozwiązań kryptograficznych. Są one jednak nieprzemyślane i świadczą o nierozumieniu występującego zjawiska elektromagnetycznego przenikania informacji związanego z sygnałami wideo i są powodem nieporozumień utrudniających rozwój metod przeciwdziałających tak groźnemu zjawisku, jakim jest bezinwazyjne pozyskiwanie informacji. Zauważmy, że w przypadku takich urządzeń, jak monitor czy drukarka niemożliwe jest zastosowanie szyfrowania treści, czyli uczynienia ich niezrozumiałymi dla człowieka, który nad nimi pracuje. Zaszyfrowanie sygnału sterującego pracą lasera drukarki [7, 9] na pewno nie umożliwi wiernego przeniesienia przetwarzanych i obserwowanych na monitorze danych na kartkę papieru.

Ponieważ stosowane metody techniczne przystosowywania urządzeń komercyjnych do zastosowań specjalnych znacznie podnoszą koszty ich nabycia, nieprzerwanie trwa proces poszukiwania nowych, tańszych rozwiązań, równie skutecznych przeciwdziałaniu infiltracji elektromagnetycznej. Najlepszym rozwiązaniem byłoby wykorzystanie urządzeń komercyjnych, w których stosowane technologie uniemożliwiałyby, mimo występowania źródeł emisji ujawniających, odtworzenie informacji przetwarzanych w sposób graficzny.

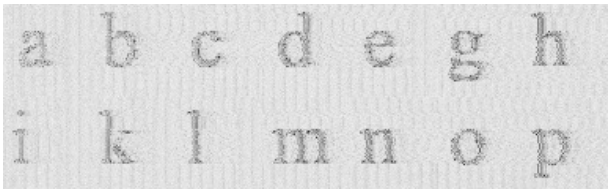
Istniało przekonanie, że jednym z takich rozwiązań jest cyfrowy standard video DVI, wykorzystywany m.in. w stacjach komputerowych. Do celów transmisji danych użytecznych oraz danych pomocniczych wykorzystywany jest w standardzie DVI protokół TMDS. W warstwie fizycznej jest to sygnał różnicowy o zminimalizowanej liczbie zmian stanów logicznych, co osiągnięto poprzez implementację odpowiednich, rozbudowanych algorytmów kodowania. Ośmiobitowe dane RGB zostają w nadajniku przetworzone na dane 10 bitowe stosując proces minimalizacji przejścia (transition minimize) oraz zrównoważenia (DC-balanced sequence). Minimalizacja liczby przejść polega na minimalizacji przejść z logicznych 0 na 1 oraz 1 na 0, które to przejścia powodują dodatkowe emisje elektromagnetyczne (transition minimization). Sygnał różnicowy oraz wspomniana minimalizacja przejść między logicznymi stanami miały zwiększyć bezpieczeństwo elektromagnetyczne przesyłanych danych. Mimo wielu publikacji w postaci artykułów i książek, takie przekonanie istnieje nadal w niektórych kręgach naukowych. Okazuje się jednak, że tak być nie musi. Standard DVI jest dobrze detektowalny, co przedstawiono na rysunku 1.

Innym przykładem rozwiązania komercyjnego uważanym za bezpieczne elektromagnetycznie jest drukarka komputerowa, w której proces naświetlania bębna światłoczułego odbywa się poprzez wykorzystanie listwy diod LED (jednym z producentów drukarek w tej technologii jest firma OKI), zamiast typowego lasera.

a)



b)



Rys.1. Przykłady odtworzonych obrazów z sygnałów emisji ujawniających dla źródła w postaci sygnału elektrycznego standardu DVI: a) font „Arial”, b) font „Times New Roman”

Rozważane zagadnienia związane z elektromagnetycznym przenikaniem informacji są niezwykle ważne. Prawidłowe rozwiązywanie pojawiających się problemów związanych z procesem infiltracji elektromagnetycznej decyduje o bezpieczeństwie wielu podmiotów oraz nas samych. Jednakże ze względu na specyfikę występujących zjawisk oraz konieczność ich rozważania w obszarze informacji niejawnych, zainteresowanych tematem ciągle brakuje.

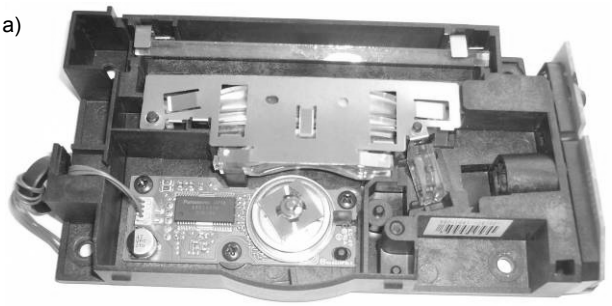
Technologia druku

Poszukiwania nowych rozwiązań związanych z technologią druku podyktowane były zapewne koniecznością zapewnienia mniejszych zapotrzebowań na energię elektryczną oraz większą niezawodnością urządzeń (mniej elementów mechanicznych). Przy tym równolegle producenci muszą mieć na uwadze spełnienie odpowiednich wymagań kompatybilności elektromagnetycznej w zakresie dopuszczalnych poziomów zaburzeń elektromagnetycznych promieniowanych i przewodzonych, których źródłem są elementy tych urządzeń oraz odporności na zaburzenia promieniowane i przewodzone, a także na wyładowania elektrostatyczne. Ponieważ są to urządzenia powszechnego użytku, producent nie ma obowiązku uwzględniać na etapie projektowania i produkcji takich urządzeń, wymagań związanych z ochroną elektromagnetyczną przetwarzanych przez te urządzenia informacji. Niemniej jednak okazuje się, że nieświadomie wykorzystywane przez producentów nowoczesne technologie np. druku, mogą stać się obiektem zainteresowań osób poszukujących prostych rozwiązań do zastosowań w obszarze skutecznego przeciwdziałania bezinwazyjnemu pozyskiwaniu informacji. Przykładem są urządzenia drukujące, będące jednym z elementów zestawów komputerowych wykorzystywanych w różnego rodzaju przedsiębiorstwach, jak i przez osoby prywatne.

Stosownym badaniom i analizom poddano dwa typy drukarek komputerowych pod kątem przydatności emisji ujawniających w procesie infiltracji elektromagnetycznej. Głównym analizowanym źródłem emisji był układ naświetlania bębna światłoczułego, czyli laser (rys.2a) i listwa diod LED (rys.2b). Analiza tych układów pokazuje, że sposób sterowania ich pracą jest odmienny. Laser drukarki sterowany jest sygnałem szeregowym i proces naświetlania bębna światłoczułego odbywa się punkt po punkcie, linia po linii.

Rejestrowany sygnał emisji ujawniającej, przy znajomości liczby punktów w linii i liczby linii w obrazie, pozwala na odtworzenie informacji wydrukowanej na papierze. Z kolei listwa diod LED sterowana jest przypuszczalnie sygnałem równoległym.

a)



b)

Rys.2. Rzeczywiste układy (a) lasera i (b) listwy diod LED stosowane w drukarkach komputerowych

Takie rozwiązanie powoduje, że źródło sygnału emisji ujawniającej jest źródłem złożonym. W tej samej chwili generowane są sygnały o zbliżonych parametrach elektrycznych (jest to analogia do drukarek wierszowych (technologia drukarek oparta jest na młoteczkach uderzających w czcionki umieszczone na obrotowym bębnie), drukujących podczas jednego obrotu bębna czcionkowego całe wiersze tekstu). W konsekwencji rejestrowany jest sygnał będący sumą wielu sygnałów emisji ujawniającej (1).

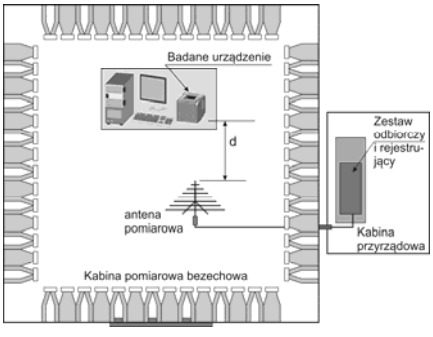
$$E_c(t) = \sum_{n=0}^{N} e_n(t), \tag{1}$$

gdzie: E_c – sygnał emisji ujawniającej dla złożonego z N diod LED źródła emisji (jednoczesne pobudzanie wszystkich diod LED w listwie), N – liczba diod LED w listwie naświetlającej bęben światłoczuły pobudzanych w tym samym czasie, e_n (n = 0, 1, …, N-1) – sygnał emisji ujawniającej dla źródła emisji w postaci pojedynczego sygnału sterującego pracą diody LED.

W takim przypadku próby odtworzenia drukowanego obrazu, zawierającego elementy graficzne czytelne dla ludzi, mogą być bezskuteczne. Czy tak jest w rzeczywistości?

Wyniki badań praktycznych

Badania sygnałów emisji ujawniających dla dwóch różnych źródeł tych sygnałów (typowa drukarka laserowa, drukarka z listwą diod LED) przeprowadzono w układzie przedstawionym na rysunku 3.



Rys.3. Układ pomiarowy w jakim prowadzono rejestrację emisji ujawniających, których źródłem były drukarki komputerowe

Współpracujący z drukarką komputer klasy TEMPEST nie był źródłem dodatkowych emisji, mogących negatywnie wpływać na uzyskane wyniki pomiarów. Zgodnie z zapisami normy NO-06-A500:2012 odległość pomiarowa d była równa 1 m. Rejestracji sygnału umożliwiającego odtworzenie informacji przeprowadzono na częstotliwościach przedstawionych w tabeli 1.

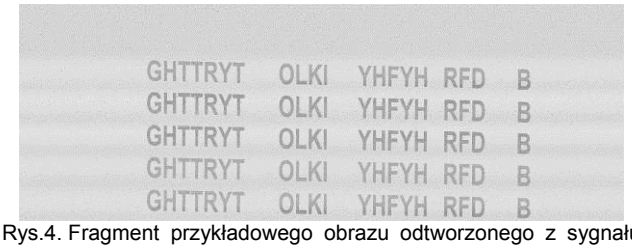
Tabela 1. Wybrane częstotliwości występowania sygnałów emisji ujawniających

	Typowa drukarka laserowa	Drukarka z listwą diod LED
Częstotliwości f_{od} występowania sygnałów emisji ujawniających [MHz]	187 MHz (BW = 10 MHz)	43 MHz (BW = 2 MHz)
	230 MHz* (BW = 10 MHz)	126 MHz (BW = 10 MHz)
	324 MHz (BW = 10 MHz)	149 MHz* (BW = 20 MHz)
	567 MHz (BW = 20 MHz)	480 MHz (BW = 50 MHz)

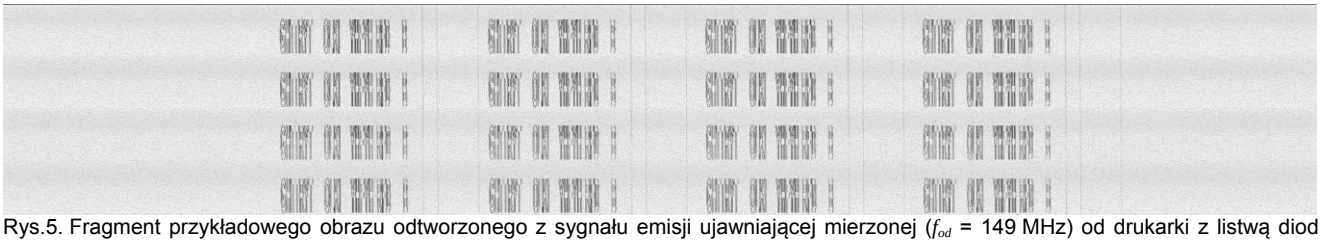
* – częstotliwości, na których dokonano próby odtworzenia graficznego przetwarzanych danych

W przypadku danych wideo, najważniejszym efektem uzyskiwanym w końcowym etapie procesu prowadzenia nasłuchu elektromagnetycznego jest odtworzenie i przedstawienie w postaci graficznej uzyskanych danych. Wynika to z faktu, że tego typu forma przedstawienia skuteczności infiltracji elektromagnetycznej jest zrozumiała i akceptowalna przez człowieka i w prosty sposób przez niego oceniana.Przykłady odtworzonych obrazów zamieszczono na rysunkach 4 i 5.

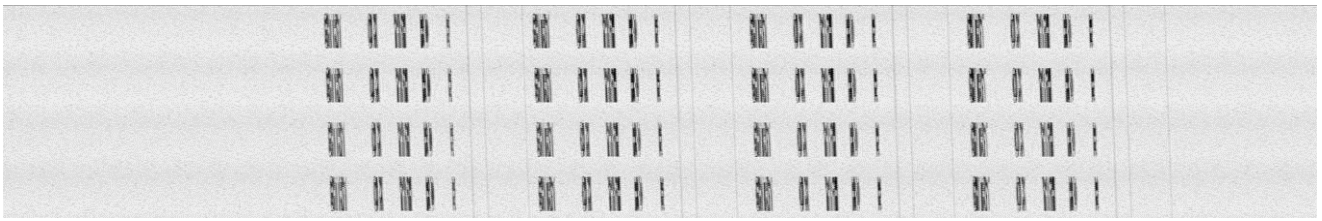
Pierwszy z nich przedstawia obraz uzyskany dla źródła emisji w postaci typowego lasera.Źródło sygnału pobudzane jest w sposób szeregowy, przez co odtworzone elementy graficzne obrazu są czytelne i akceptowalne dla człowieka. Obraz zwiera pojedynczy drukowany arkusz.



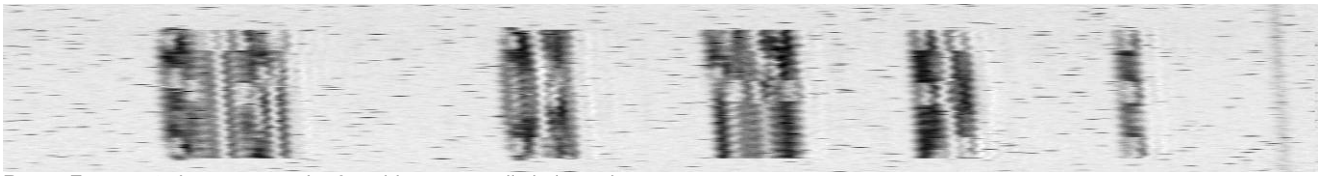
Rys.4. Fragment przykładowego obrazu odtworzonego z sygnału emisji ujawniającej (f_{od} = 230 MHz) typowej drukarki laserowej (inwersja obrazu, rozmiar znaków: 28 pkt)



Rys.5. Fragment przykładowego obrazu odtworzonego z sygnału emisji ujawniającej mierzonej (f_{od} = 149 MHz) od drukarki z listwą diod LED (inwersja obrazu, rozmiar znaków: 28 pkt)



Rys.6. Fragment przykładowego obrazu odtworzonego z sygnału emisji ujawniającej mierzonej (f_{od} = 149 MHz) od drukarki z listwą diod LED (inwersja obrazu, rozmiar znaków: 14 pkt)



Rys.7. Fragment obrazu z rysunku 6 poddany operacji skalowania

Z kolei na rysunku 5 przedstawiono obraz dla źródła w postaci listwy diod LED. Zawiera on fragmenty czterech drukowanych arkuszy. Świadczy to o tym, że listwa diod LED może zawierać cztery szeregi diod sterowanych szeregowo tym samym sygnałem elektrycznym. Ponadto, każdy szereg diod może być pobudzany szeregowo w sposób sekwencyjny (szereg diod dzielonych jest na kilka sekcji) sygnałem ciągłym, a nie impulsowym, jak ma to miejsce w typowych drukarkach laserowych. W takim przypadku wydruk poziomej czarnej linii związany jest z ciągłym sygnałem sterującym, o stałej amplitudzie i czasie trwania odpowiadającym długości linii. Dla typowego lasera jest to sygnał impulsowy związany z każdym punktem rysowanej linii. W wyniku takiego sterowania pracą lasera w odtworzonych elementach graficznych obrazów otrzymujemy ich wypełnienie (rysunek 4), czego nie zauważamy dla drukarek z listwą diod LED. Dla tego typu drukarek możemy zauważyć jedynie krawędzie pionowe i ukośne znaków (rysunek 5), przez co stają się one mało czytelne i trudno rozpoznawalne (dla znaków o rozmiarze 28 pkt).

Na rysunkach 6 i 7 przedstawiono dodatkowo fragment odtworzonego obrazu dla źródła w postaci listwy diod LED i rozmiaru znaków 14 pkt, zbliżonego do powszechnie używanego rozmiaru 12 pkt. Odczyt znaków, nawet po przeprowadzonych modyfikacjach, jest niemożliwy.

Należy zauważyć, że poziomy emisji elektromagnetycznych mierzonych od analizowanych drukarek są zbliżone. Świadczy to również o tym, że mogące wystąpić poziomy sygnałów emisji ujawniających, aby były bezpieczne nie muszą być redukowane do minimum. Przede wszystkim muszą być redukowane do

minimum występujące cechy dystynktywne mierzonych emisji ujawniających. Jednak, podobnie jak w przypadku standardu cyfrowego DVI, tak i w przypadku drukarek z listwą diod LED, pożądanego efektu nie osiągnięto. Spowodowane to jest brakiem czysto równoległego przetwarzania sygnału wideo, który steruje pracą diod LED. Sygnał użyteczny przypuszczalnie jest sygnałem równolegle-szeregowym. Wówczas:

$$E_s(t) = \sum_{n=0}^{k-1} e_n(t), \tag{2}$$

$$k = \frac{N}{d}, \tag{3}$$

gdzie: E_s – sygnał emisji ujawniającej dla złożonego z k diod LED źródła emisji (jednoczesne pobudzanie k diod LED w listwie), k – liczba diod LED pojedynczej sekcji pobudzanych równolegle (w tym samym czasie), d – liczba sekcji sterowanych szeregowo.
Powoduje to, że emisja ujawniająca skorelowana z takim źródłem posiada pewne cechy dystynktywne sygnału pierwotnego. Brak wyraźnych takich cech możemy zauważyć w przypadku znaków o rozmiarze 14 pkt, czyli zbliżonym do powszechnie stosowanego rozmiaru znaków fontów komputerowych. Wówczas odczyt, a tym samym bezinwazyjne pozyskanie informacji w przeciwieństwie do typowej drukarki laserowej, staje się bardzo utrudniony.

Podsumowanie

W artykule przedstawiono wyniki badań i analiz emisji ujawniających, których źródłami są drukarki komputerowe wykorzystujące technologię druku opartą na typowym laserze oraz listwie diod LED. Celem prowadzonych analiz było pokazanie wpływu różnic rozwiązań konstrukcyjnych urządzeń drukujących na skuteczność procesu infiltracji elektromagnetycznej, a tym samym możliwości ich wykorzystania w obszarze ochrony przetwarzanych informacji (drukowanych) przed elektromagnetycznym przenikaniem.

Druk oparty na technologii laserowej wykorzystuje sygnał szeregowy sterujący pracą lasera. Takie rozwiązanie powoduje, że sygnał emisji ujawniającej posiada wyraźne cechy dystynktywne odpowiadające pierwotnemu sygnałowi sterującemu. Obraz odtworzony metodą rastrowania (przy znajomości parametrów: jakości druku (rozdzielczości), liczby drukowanych stron na minutę) ukazuje wprost elementy graficzne drukowanych dokumentów. Są one wyraźne i w większości przypadków nie wymagają stosowania dodatkowych metod cyfrowego przetwarzania obrazów mających na celu ich uwydatnienie.

W przypadku drukarek wykorzystujących w procesie naświetlania bębna światłoczułego listwę diod LED, sygnał emisji ujawniającej nie posiada tak wyraźnych cech skorelowania z pierwotnym sygnałem sterującym pracą listwy. Elementy graficzne zawarte w odtworzonym obrazie wymagają stosowania dodatkowych zabiegów, przede wszystkim operacje skalowania, poprawiających percepcję obrazów. Ostatecznie elementy zawarte w obrazie mogą być rozpoznawalne (rozmiar znaków 28 pkt). Niemniej jednak czytelność zawartych w obrazie znaków jest dużo mniejsza niż dla obrazów uzyskiwanych z sygnałów emisji ujawniających pochodzących od typowych drukarek laserowych.

LITERATURA

[1] Kubiak I., Digital processing methods of images and signals in electromagnetic infiltration process, *Image Processing and Communication*, vol.18, no. 1, 2014

[2] Kubiak I., The unwanted emission signals in the context of the reconstruct possibility of data graphics, *International Journal of Image, Graphics and Signal Processing*, 11/2014

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

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

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

[6] Kubiak I., Font komputerowy odporny na proces infiltracji elektromagnetycznej, *Przegląd Elektrotechniczny*, 6/2014, strony 207-215

[7] Grzesiak K., Przybysz A., Emission security of laser printers, *Military Communications and Information Systems Conference, Wrocław 2010*, (Concepts and Implementations for Innovative Military Communications and Information Technologies, Wydawnicto WAT 2010, ISBN 978-83-61486-70-1, strony 353-363

[8] Przybysz A., Bezpieczeństwo emisji interfejsów DVI i HDMI, *Przegląd Telekomunikacyjny, Wiadomości Telekomunikacyjne*, 7/2014, strony 669 - 673

[9] Grzesiak K., Przybysz A., Programowy generator rastra, *Przegląd Telekomunikacyjny, Wiadomości Telekomunikacyjne*, 11/2011, strony 1596-1600

[10] Kubiak I., Musiał S., Sprzętowy generator rastra jako narzędzie wspomagające infiltrację elektromagnetyczną, *Przegląd Telekomunikacyjny, Wiadomości Telekomunikacyjne*, 11/2011, strony 1601-1607

[11] Kubiak I., Przybysz A., Ochrona elektromagnetyczna systemów i sieci teleinformatycznych, *Przegląd Telekomunikacyjny, Wiadomości Telekomunikacyjne*, 12/2006, strony 371-374

[12] Janulewicz A., Pawelec J., Odtwarzanie informacji z części widma sygnału emisji ujawniającej monitora ekranowego, *Krajowa Konferencja Radiokomunikacji Radiofonii i Telewizji - KKRRiT 2005*, Kraków, strony 119-122

[13] Kuhn *Markus* G., Compromising emanations: eavesdropping risks of *computer* displays, *Technical reports published by the University of Cambridge Computer Laboratory 2003*

[14] Kuhn Markus G., Optical Time-Domain Eavesdropping Risks of CRT Displays, *Proceedings 2002 IEEE Symposium on Security and Privacy*, Berkeley, California, 12–15 May 2002, IEEE Computer Society, pp. 3–18, ISBN 0-7695-1543-6

[15] Loughry J., Umphress David A., Information Leakage from Optical Emanations, *ACM Transactions on Information Systems Security*, Vol. 5, No. 3, pp. 262–289, August 2002

***Autorzy**: dr inż. Ireneusz Kubiak, Wojskowy Instytut Łączności, ul. Warszawska 22A, 05-130 Zegrze Południowe, E-mail: i.kubiak@wil.waw.pl, mgr inż. Artur Przybysz, Wojskowy Instytut Łączności, ul. Warszawska 22A, 05-130 Zegrze Południowe, E-mail: a.przybysz@wil.waw.pl*