**Ireneusz KUBIAK**
Wojskowy Instytut Łączności

doi:10.15199/48.2017.06.25

# Sieć zasilania źródłem emisji wrażliwych pochodzących od drukarek laserowych

***Streszczenie:*** *Drukarki laserowe jako urządzenia elektroniczne stają się źródłem emisji elektromagnetycznych. Najczęściej mamy na uwadze emisje promieniowane, które mogą być wykorzystane w bezinwazyjnym pozyskiwaniu informacji przetwarzanych (drukowanych) przez te urządzenia. Urządzenia drukujące są również źródłem emisji przewodzonych, które posiadają cechy drukowanych danych. Podobnie jak emisje promieniowane mogą być one wykorzystane do przechwytu informacji.*

***Abstract:*** *A laser printer as a electronic device is a source of a electromagnetic emissions. Very often we think about a radiated emissions which we could use in a non-invasive acquisition of a classified information. Unfortunately the device is the source of a conducted emissions. The emissions have a characteristics correlated with the data printing. The conducted emissions could be used to reconstruct of the sensitive information in the same way as the radiated emissions. (**A power line as a source of sensitive emissions from laser printers**)*

**Słowa kluczowe:** emisje wrażliwe, sieć zasilania, drukarka laserowa
**Keywords:** sensitive emission, power line, laser printer

## Wstęp

Ochrona danych występujących pod każdą postacią, elektroniczną czy też papierową, stanowi w obecnych czasach ogromne wyzwanie. W wielu dziedzinach życia okazuje się, że stosowanie nawet najbardziej wyszukanych rozwiązań nie stanie się skuteczne jeśli zawiedzie człowiek, jako najsłabsze ogniwo. Niemniej jednak zakłada się, że człowiek przestrzega wszelkich reguł, a ochronę informacji zapewniamy poprzez stosowanie rozwiązań, mających na celu ograniczenie możliwości pozyskiwania danych metodami bezinwazyjnymi. Obszar zagadnień związanych z ochroną danych, występujących pod postacią różnego rodzaju przebiegów elektrycznych, jest bardzo szeroki. Materiał zawarty w artykule nie obejmuje całościowo zagrożeń wynikających z elektromagnetycznego przenikania informacji. Jest jedynie zwróceniem szczególnej uwagi na jeden z elementów bezpieczeństwa systemów i sieci teleinformatycznych, którym jest bezpieczeństwo danych, które mogą być ujawnione w wyniku wystąpienia ich w postaci niepożądanych emisji przewodzonych.

Poza ochroną informacji metodami kryptograficznymi oraz organizacyjnymi bardzo często wykorzystuje się metody, których zadaniem jest ograniczenie rozprzestrzeniania się różnego rodzaju emisji (promieniowanych i przewodzonych). Emisje pochodzące od urządzeń wykorzystujących prąd elektryczny bardzo często posiadają cechy, które z łatwością mogą ujawnić przetwarzane dane, występujące w postaci sygnałów elektrycznych. Stosowanie w ochronie informacji nawet najbardziej wyszukanych rozwiązań kryptograficznych nie ogranicza powstających zjawisk elektromagnetycznego przenikania informacji. Przekonanie, że techniki kryptograficzne mogą przeciwdziałać powyższemu zjawisku jest błędne. Dowodem na to niech będzie chociażby konieczność badań urządzeń kryptograficznych pod kątem możliwości wystąpienia elektromagnetycznego „wycieku" informacji i ich odtworzenia na bazie zarejestrowanego sygnału ujawniającego. Sygnału, który występuje w postaci jawnej przed poddaniem go procesowi utajnienia.

Najczęściej mówi się o zagrożeniach jakie niosą ze sobą emisje ujawniające typu promieniowanego. Mogą być one traktowane jak typowe emisje radiowe, których odbiór i odpowiednie przetworzenie pozwala na wyświetlenie w czasie rzeczywistym danych np. wyświetlanych na monitorze znajdującym się kilkadziesiąt metrów od receptora emisji. Zrozumiałym jest, że dane te nie mogą być chronione kryptograficznie, gdyż muszą posiadać postać zrozumiałą dla człowieka. Obserwacja emisji ujawniających w czasie rzeczywistym jest możliwa dzięki wielokrotnemu powtarzaniu sygnału (np. odświeżanie obrazu monitora ekranowego), będącego źródłem emisji niepożądanych. Jednak nie tylko tego typu dane narażone są na ich ujawnienie. Pojedyncze sygnały elektryczne również mogą być groźne z punktu widzenia skuteczności tzw. „nasłuchu" elektromagnetycznego. Przykładem takich sygnałów mogą być sygnały użyteczne, wymuszające pracę układów laserowych drukarek wykorzystywanych w procesie naświetlania bębna światłoczułego.

W każdym z ww. przypadków, celem eliminacji lub zmniejszenia znaczenia występujących emisji wykorzystuje się szereg metod, które przy uwzględnieniu właściwości różniczkujących Kanału Przenikania Informacji (KPI) uniemożliwiają pozyskanie danych tą drogą. Do metod tych zalicza się ekranowanie, transmisję różnicową sygnałów elektrycznych, uziemiane, wykorzystanie koralików ferrytowych.

W wielości możliwych rozwiązań nie należy jednak zapominać o niepożądanych emisjach skorelowanych z przetwarzanymi danymi, które mogą pojawić się w przewodach zasilania od strony źródła tych emisji. Bardzo istotnym jest fakt, że odległości ich rozprzestrzeniania się w wielu przypadkach mogą okazać się dużo większe niż dla emisji promieniowanych. Dlatego emisje przewodzone są również ważnym obiektem badań i zabezpieczeń przed niekontrolowanym „ulotem" informacji.

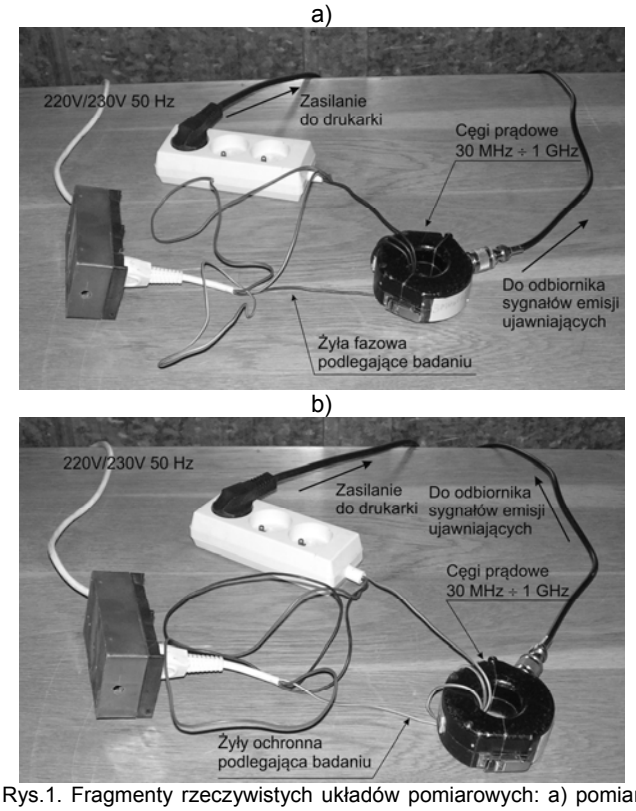
W artykule przedstawiono wyniki badań i przykłady odtworzonych obrazów dla źródła emisji przewodzonych w postaci drukarki laserowej, które jednoznacznie pokazują występujące zagrożenie. Zwrócono uwagę na zależność skuteczności procesu infiltracji elektromagnetycznej od żyły (fazowa (*L*), neutralna (*N*) i ochronna (*PE*)) przewodu wykorzystywanej w „podsłuchu" elektromagnetycznym. Badania przeprowadzono na dwóch żyłach: fazowej i ochronnej. Analizę oparto na obiektywnej ocenie wzrokowej uzyskiwanych obrazach, zawierających elementy graficzne przetwarzanych danych tekstowych, pisanych fontami tradycyjnym („Arial") i bezpiecznymi („Bezpieczny Symetryczny", „Bezpieczny Niesymetryczny" i „Bezpieczny Prosty" [3, 4]).

## Warunki prowadzonych testów

Stosownym badaniom i analizom wzrokowym poddano sygnały emisji przewodzonych, których źródłem była

drukarka laserowa oparta na technologii listwy LED, jako układu naświetlającego bęben światłoczuły. Niemniej jednak, wyniki przeprowadzonych analiz nie należy utożsamiać tylko z drukarkami tego typu. Urządzenia drukujące, w których wykorzystywany jest układ naświetlania bębna światłoczułego oparty na układzie jedno- i dwudiodowym jest analogicznym źródłem emisji przewodzonych. W przypadku tych urządzeń również i one stają się groźne z punktu widzenia nieświadomej utraty informacji. Poziom tego zjawiska zależy jednak od jakości druku (z oszczędnością tonera lub z jego brakiem), w przeciwieństwie do drukarek wyposażonych w listwę LED.

W trakcie badań receptorem emisji były cęgi prądowe, pracujące w zakresie częstotliwości od 30 MHz do 1 GHz. Jako medium transmisyjne generowanych emisji przewodzonych wykorzystano trzyżyłowy przewód (rys.1). Cęgi umieszczono na linii *L* i *PE* oraz na wszystkich trzech liniach jednocześnie (w linii *N* brak było mierzalnych emisji niepożądanych). Pozwoliło to sklasyfikować poszczególne linie pod kątem ich przydatności jako źródeł emisji wrażliwych i wykorzystania ich w procesie zwanym atakiem typu TEMPEST[1].




Rys.1. Fragmenty rzeczywistych układów pomiarowych: a) pomiar sygnału w linii fazowej przewodu elektrycznego, b) pomiar sygnału w linii ochronnej przewodu elektrycznego

Badania przeprowadzono dla kilku wartości szerokości pasma pomiarowego (*BW*, ang. BandWidth): 500 kHz, 2 MHz, 20 MHz. Podyktowane to było uzyskiwaniem różnej jakości sygnałów, a tym samym odtwarzanych obrazów poddawanych analizie wzrokowej. Wydruki były wykonywane z rozdzielczością (tryb pracy) 1200 dpi x 1200 dpi (ang. dots per inch) dla opcji „Best" i „Eco" („Best" – opcja bez oszczędności tonera, „Eco" – opcja oszczędności tonera).

[1] TEMPEST – ang. temporary emanation and spurious transmission. Nazwa nadana programowi ochrony przed niekontrolowaną emisją ujawniającą, który powstał w latach 50-tych w USA na zlecenie Pentagonu

Niezależnie od typu rejestrowanych emisji ujawniających, do odtworzenia danych przetwarzanych w drukarce niezbędne są informacje o długości pojedynczej linii wydruku oraz o liczbie linii zawartych na pojedynczej kartce wydruku. W przeciwieństwie do map bitowych uzyskiwanych z sygnałów emisji ujawniających skorelowanych z pracą monitorów komputerowych, odtwarzane obrazy z sygnałów emisji dla źródeł w postaci drukarek laserowych wymagają większych zasobów pamięciowych. Dla przykładu obecnie stosowane drukarki laserowe umożliwiają wydruk w standardowym trybie 1200 dpi x 1200 dpi. Jeżeli przyjmiemy stronę wydruku o formacie A4, obszar wydruku wynosi 8,27 cala x 11,69 cala, co odpowiada obrazowi o wymiarach 9 924 x 14 028 punktów. Ponadto, biorąc pod uwagę, że w rejestrowanym sygnale każdemu punktowi wydruku powinny odpowiadać około 3 próbki sygnału, mamy do czynienia z mapami bitowymi o wymiarach 29 772 x 14 028 pikseli, co odpowiada ciągom danych o wielkości około 417 MB.

Istotnym parametrem badań jest wykorzystywane pasmo pomiarowe. Jego szerokość musi być odpowiednia do rejestrowanych sygnałów. Zbyt szerokie pasmo może powodować utratę jakości odtwarzanego obrazu ze względu na jego silne zaszumienie. Wąskie pasmo, może wpływać na utratę istotnych cech sygnału, które mogą decydować nie tylko o odtworzeniu danych, ale również o ich odczycie.

Zgrubnego oszacowania poszukiwanych parametrów sygnałów można dokonać w oparciu o dane katalogowe dotyczące szybkości wydruku poszczególnych modeli drukarek laserowych. W tym celu do wyznaczania pasma podstawowego sygnału sterującego laserem podczas wydruku jednego punktu można posłużyć się poniższym wzorem:

$$B = \frac{szer \cdot dl \cdot dpi^2}{t_{1str}} \tag{1}$$

gdzie: *B* – pasmo sygnału przy wydruku jednego punktu (w Hz); *szer* – szerokość obszaru wydruku w calach (dla strony A4 i marginesach równych 1 cal *szer* = 6,27 cala); *dl* – długość obszaru wydruku w calach (dla strony A4 i marginesach równych 1 cal, *dl* = 9,69 cala); *dpi* – ustawiona rozdzielczość podczas drukowania (ilość punktów na cal); $t_{1str}$ – czas wydrukowania jednej strony.

Jeżeli przyjmiemy, że urządzenie drukujące pracuje w trybie 1200 dpi x 1200 dpi i drukuje około 35 stron na minutę, można oszacować, że czas wydruku 1 strony wynosi $t_{1str}$ = 1,71 s. Przy założeniu, że drukowana jest strona formatu A4 oraz ustawione są typowe marginesy (górny, dolny, lewy, prawy) wielkości 1 cala, liczba drukowanych punktów na takiej powierzchni wynosi 87 489 072, a więc czas wydrukowania jednego punktu jest równy $1{,}95 \cdot 10^{-8}$ sekundy. Na podstawie tych obliczeń i zależności (1) pasmo sygnału sterującego laserem podczas drukowania jednego punktu wynosi *B* = 51 163 200 Hz.

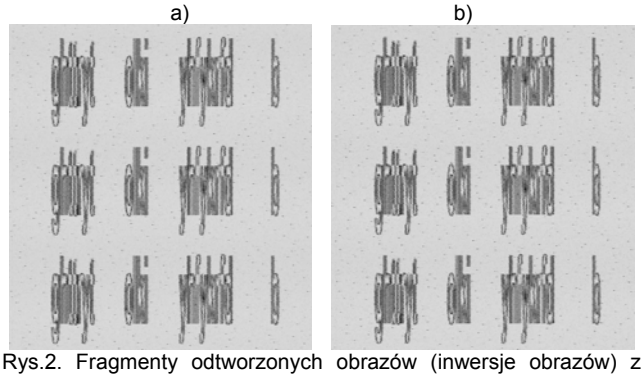
W rzeczywistości pasmo sygnału sterującego pracą diody laserowej może różnić się znacząco od oszacowanego zgodnie z powyższą zależnością i jest zależne od konstrukcji i trybu pracy drukarki (liczba diod laserowych, wydruk tekstu lub grafiki) i należy go dobierać doświadczalnie celem uzyskania jak najlepszego obrazu.

**linie zasilające jako medium transmisyjne emisji wrażliwych**

Urządzenia zasilane prądem elektrycznym są źródłem nie tylko emisji promieniowanych, ale także emisji przewodzonych. Te drugie są na tyle groźne, że można je mierzyć niemal w każdym gniazdku zasilającym, znajdującym się na tej samej linii co gniazdko zasilające w

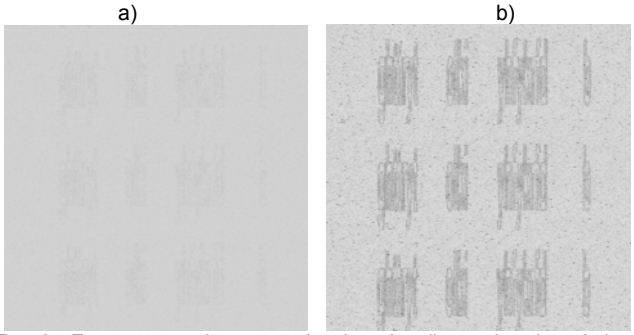
prąd elektryczny urządzenie przetwarzające informacje. Należy jednak zauważyć, że nie każda linia przewodu elektrycznego jest takim samym nośnikiem emisji ujawniających. Przeprowadzone badania drukarki LED pokazują, że najmniej skuteczną jest linia *N*. Najskuteczniejszą linią jest z kolei linia fazowa *L* (rys.2÷4).

Jednak należy zaznaczyć, że nie jest to regułą, a zjawisko to zależy od typu drukarki. Wynika to z faktu, iż producenci urządzeń drukujących stosują różne rozwiązania układów filtrujących sieć zasilania. Zatem kwalifikacji drukarki należy dokonać po uprzednim przeprowadzeniu stosownych testów, których wyniki pozwolą na ocenę występujących emisji wrażliwych np. zgodnie z dokumentami SDIP-27/1 „NATO Tempest Requirements and Evaluation Procedures" lub SDIP-28/1 „NATO Zoning Procedures".



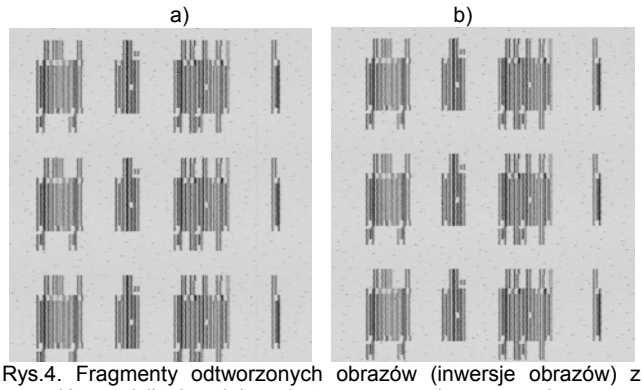

Rys.2. Fragmenty odtworzonych obrazów (inwersje obrazów) z sygnałów emisji ujawniających typu przewodzonego, mierzonego w linii fazowej przewodu elektrycznego: a) opcja „Best", b) opcja „Eco" (częstotliwość odbioru $f_o$ = 224 MHz, częstotliwość próbkowania $f_s$ = 62 MHz, pasmo odbioru *BW* = 20 MHz)

Jednym z istotnych parametrów charakteryzujących sygnał jest jego moc. Jednak w przypadku sygnałów niepożądanych nie zawsze moc sygnału może klasyfikować go jako przydatnego do dalszych analiz, z punktu widzenia skuteczności nasłuchu elektromagnetycznego. Spowodowane jest to np. występowaniem silnych sygnałów zakłócających związanych z prawidłową pracą urządzeń (np. sygnały synchronizacji pionowej lub poziomej monitorów komputerowych, silniki krokowe lub grzałka drukarek laserowych). Dlatego bardzo często podstawą analiz obrazów w procesie infiltracji elektromagnetycznej jest analiza wzrokowa.




Rys.3. Fragmenty odtworzonych obrazów (inwersje obrazów) z sygnałów emisji ujawniających typu przewodzonego, mierzonego w linii ochronnej przewodu elektrycznego, podczas pracy urządzenia drukującego z opcją „Best": a) częstotliwość odbioru $f_o$ = 224 MHz, b) częstotliwość odbioru $f_o$ = 195 MHz (częstotliwość próbkowania $f_s$ = 62 MHz, pasmo odbioru *BW* = 20 MHz)

Dotyczy to oczywiście przypadków, kiedy nasłuchowi elektromagnetycznemu podlegają tory wideo urządzeń o przeznaczeniu specjalnym. Tego typu analiza, bazując na doświadczeniu operatora, przynosi bardzo dobre wyniki i pozwala w wysokim procencie podejmować właściwe decyzje.




Rys.4. Fragmenty odtworzonych obrazów (inwersje obrazów) z sygnałów emisji ujawniających typu przewodzonego, mierzonego w linii fazowej przewodu elektrycznego (tekst pisany fontem „Bezpieczny Niesymetryczny"): a) opcja „Best", b) opcja „Eco" (częstotliwość odbioru $f_o$ = 224 MHz, częstotliwość próbkowania $f_s$ = 62 MHz, pasmo odbioru *BW* = 20 MHz)

Zwróćmy jednak uwagę na wartość wspomnianego parametru dla przypadków rozpatrywanych powyżej pozbawionych silnych zakłóceń (rys.2, 3 i 4). Sygnał *y*, dla którego określa się moc średnią zgodnie z zależnością:

$$P_y = \frac{1}{K}\sum_{k=0}^{K-1} y^2(k) \tag{2}$$

lub dla obrazu uzyskanego z sygnału *y* metodą rastrowania:

$$P_b = \frac{1}{N \cdot M}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} y^2(j,i) \tag{3}$$

gdzie: $K = N \cdot M$ – liczba próbek sygnału *y*, *P* – moc średnia sygnału *y*, *M* – liczba kolumn obrazu, *N* – liczba wierszy obrazu,
rozpatruje się w obszarze od pierwszej do ostatniej próbki (piksela) sygnału (obrazu uzyskiwanego metodą rastrowania). Wartości mocy średniej obliczone zgodnie z (3) dla sygnałów budujących obrazy przedstawione na rys.2, 3 i 4 zawarto w tabeli 1.

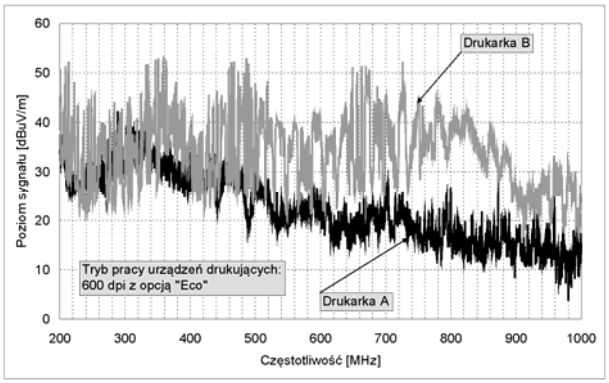
Tabela 1. Wartości mocy średniej sygnałów budujących obrazy zamieszczone na rys.3, 4 i 5

| Obraz | | Wartość mocy średniej |
|---|---|---|
| Rysunek 3 | a | 4557,95 |
| | b | 4887,91 |
| Rysunek 4 | a | 2155,01 |
| | b | 2857,75 |
| Rysunek 5 | a | 5415,86 |
| | b | 4995,72 |

**Emisje promieniowane**

Wspomniano, że istotne znaczenie w infiltracji elektromagnetycznej urządzeń, przetwarzających dane niejawne mają emisje promieniowane. Mogą być one skutkiem występujących emisji przewodzonych, które powstają w wyniku przetwarzania danych istniejących w postaci przebiegów elektrycznych. Można zatem twierdzić, że brak niepożądanych emisji przewodzonych skutkuje brakiem występowania emisji promieniowanych. Twierdzenie odwrotne również może być słuszne. Niemierzalne emisje promieniowane świadczą o skutecznym filtrowaniu emisji przewodzonych, które nie są wówczas źródłem wrażliwych emisji promieniowanych. W zakresie zależności między dwoma rodzajami emisji promieniowanej i przewodzonej przeprowadzono odpowiednie badania, którym poddano drukarkę LED

oznaczoną jako A oraz drukarkę wyżej analizowaną oznaczoną jako B. Testy wykonano w zakresie częstotliwości od 200 MHz do 1000 MHz, w którym najczęściej występują emisje wrażliwe typu promieniowanego o poziomach, umożliwiających skuteczne prowadzenie infiltracji elektromagnetycznej. Uzyskane wyniki przedstawiono na rys.5. Rejestrowane poziomy emisji elektromagnetycznych (również emisji ujawniających) dla drukarki A są dużo niższe od poziomów rejestrowanych dla drukarki B.




Rys.5. Zaburzenia promieniowane mierzone w zakresie częstotliwości 200 MHz ÷ 1000 MHz od drukarek A i B, pracujących w trybie 600 dpi x 600 dpi z oszczędnością tonera (opcja „Eco"), pasmo pomiarowe *BW* = 1 MHz

Drukarka A poddana była również badaniom w zakresie potencjalnego źródła emisji przewodzonych. Wyniki tych badań nie wykazały jednak podatności urządzenia na infiltrację elektromagnetyczną. Brak lub bardzo niski poziom niepożądanych emisji przewodzonych uniemożliwiał zarejestrowanie odpowiednich realizacji sygnałów a tym samym pozyskanie informacji drogą bezinwazyjną. Potwierdzenia tego zjawiska można dopatrywać się w tym, że badane urządzenie nie jest również źródłem promieniowanych emisji niepożądanych (rys.5), niezależnie od testowanej linii zasilającej.

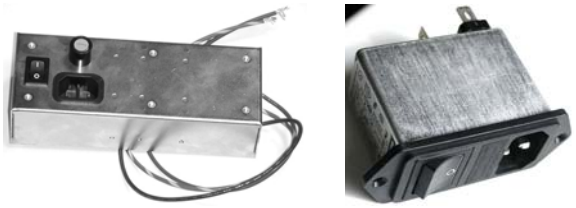

Rys.6. Przykład przebiegu czasowego sygnałów różnicowych sterujących pracą układu naświetlania bębna światłoczułego (głowicy LED, drukarka A)

Znaczący wpływ na obserwowane zjawisko może mieć stosowany przez producenta system sterowania pracą głowicy LED. W przypadku tej drukarki wykorzystano transmisję różnicową (rys.6) sygnałów, pod postacią których występuje przetwarzana (drukowana) informacja. Jest to rozwiązanie, które dedykowane jest przede wszystkim dla zwiększenia odporności systemów na zaburzenia zewnętrzne. Niemniej jednak wpływa ono również na redukcję zaburzeń wytwarzanych przez taki układ. Wyraźnie widać to na rys.5, co również ma ogromne znaczenie w obniżaniu skuteczności układu jako źródła potencjalnych emisji wrażliwych.

**Rozwiązania układów zasilających**

Brak emisji przewodzonych, a tym samym emisji promieniowanych, jest m.in. skutkiem odpowiedniej filtracji obwodów zasilających. Podstawowy układ zasilający, wprowadzający wystarczające tłumienie sygnałów emisji niepożądanych, musi bazować na odpowiednich filtrach sieciowych, których skuteczność może być potwierdzana m.in. poprzez pomiar emisji promieniowanych (rys.5) i przewodzonych.

W przypadku niedostatecznej tłumienności typowych układów zasilających, stosowanych w rozwiązaniach komercyjnych, mogą być wykorzystane dodatkowe układy filtrujące (rys.7, 1- i 3-fazowe, na prądy od 6 A do 20 A), często wyposażone w gniazdo IEC. Takie rozwiązania są implementowane w konstrukcjach urządzeń specjalnych [5], zapewniając tłumienie sygnałów niepożądanych na poziomie 80 dB, już od częstotliwości 100 kHz.



Rys.7. Przykładowe układy filtrujące linię zasilającą

Nie zawsze w rozwiązaniu konstrukcyjnym jest odpowiednia przestrzeń do montażu dodatkowych, bardzo często niemałych, elementów elektronicznych, np. filtrów sieciowych. Są one wówczas montowane na zewnątrz urządzenia, zmieniając jego wygląd (rys.8), często nie akceptowalny przez użytkownika. Obecne rozwiązania filtracji obwodów zasilania, ze względu na możliwości ich miniaturyzacji, implementowane są bezpośrednio w urządzeniu, przez co i jego wygląd pozostaje niezmieniony.

Rys.8. Przykład montażu filtra sieciowego przeciwzakłócającego w urządzeniu drukującym, zapewniającym ochronę elektromagnetyczną drukowanych danych

**Podsumowanie**

Dotychczas przeprowadzone analizy, bazujące na emisjach ujawniających typu promieniowanego kazały uświadomić sobie, jakie zagrożenie niesie ze sobą

używanie urządzeń niezabezpieczonych przed infiltracją elektromagnetyczną. Przy tym wykazano, że jedną z metod przeciwdziałających wspomnianemu procesowi jest wykorzystanie fontów bezpiecznych. Podobne wnioski można wyciągnąć w przypadku emisji ujawniających typu przewodzonego.

Przeprowadzone testy drukarki B pokazały, jak istotnym elementem w ochronie elektromagnetycznej przetwarzanych informacji jest linia zasilająca. Występujące emisje są na tyle silne, że rejestrowane sygnały pozwalają na odtworzenie danych w postaci obrazów, zawierających elementy graficzne znaków drukowanych przez drukarkę laserową. Stosowanie w edycji tekstu fontów bezpiecznych zwiększa odporność urządzenia na podsłuch elektromagnetyczny, w którym wykorzystywane są emisje przewodzone.

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

LITERATURA

[1] Grzesiak K., Kubiak I., Musiał S., Przybysz A., *Elektromagnetyczne bezpieczeństwo informacji*, Wydawnictwo WAT 2009, ISBN 978-83-61486-32-9;

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

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

[5] 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, Wydawnictwo WAT 2010, ISBN 978-83-61486-70-1, strony 353-363

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

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

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

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

[10] 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

[11] Kubiak I., Przybysz A., *Konstrukcyjne rozwiązania urządzeń komercyjnych w aspekcie ochrony elektromagnetycznej przetwarzanych informacji,* Przegląd Elektrotechniczny 11/2015, doi:10.15199/48.2015.11.12

[12] Kubiak I., Przybysz A., Technologia druku a elektromagnetyczna ochrona informacji, *Przegląd Elektrotechniczny,* nr 1/2016, DOI: 10.15199/48.2016.01.42

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

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

[15] Nidhi Chandra, Amnesh Goel, "*A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise Of RGB Values and Explosive Inter-Pixel Displacement*", I.J. Image, Graphics and Signal Processing,2/2012, 16-22, DOI: 10.5815/ijigsp.2012.02.03

[16] Bahare Jalilian, Abdolah Chalechale, "*Persian Sign Language Recognition Using Radial Distance and Fourier Transform*", I.J. Image, Graphics and Signal Processing,1/2014, 40-46, DOI: 10.5815/ijigsp.2014.01.06

[17] Nilima Kulkarni, Color Thresholding, "*Method for Image Segmentation of Natural Images*", I.J. Image, Graphics and Signal Processing,1/2012, 28-34, DOI: 10.5815/ijigsp.2012.01.04

[18] Deok J. Park, Kwon M. Nam: "*Multiresolution Edge Detection Techniques, Pattern Recognition"*, Vol. 28, 1995

[19] Michael J. McCarthy, *The Pentagon worries that spies can see its computer screens, someone could watch what's on your VDT"*, The Wall Street Journal, 07.08.2000

[20] Allen R. L., "*Signal Analysis: Time, Frequency, Scale, and Structure"*, 2004

[21] Hong Zeng, "*Dual image processing algorithms and parameter optimization"*, Seventh International Conference on Natural Computation (ICNC), Shanghai 2011, Conference materials volume 2, p.946-950, ISSN 2157-9555