E-ISSN 2544-9567
ISSN 1230-3801

Zeszyt 170 nr 3/2024, str. 65- 81
Volume 170 No. 3/2024, pp. 65 - 81

WYCIEK INFORMACJI POPRZEZ INFILTRACJĘ ELEKTROMAGNETYCZNĄ I CZYNNIKI WARUNKUJĄCE JEJ POWODZENIE

LEAKING OUT OF INFORMATION DUE TO ELECTROMAGNETIC INFILTRATION AND ITS FAVOURABLE CIRCUMSTANCES

Marian WNUK, *marian.wnuk@wat.edu.pl,* ORCID: 0000-0003-4576-4023
Konrad SZCZEPANKIEWICZ, *konrad.szczepankiewicz@wat.edu.pl*,
ORCID: 0000-0003-3292-8113
Wojskowa Akademia Techniczna, ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
Military University of Technology, 2 Kaliskiego St., 00-908 Warsaw, Poland

DOI 10.5604/01.3001.0054.7455

Streszczenie: Urządzenia elektroniczne stanowią nieodzowny element współczesnej cywilizacji. Przetwarzają one rozmaite spektrum informacji (od rozrywkowych, poprzez dane medyczne i militarne, aż do ważnych spraw państwowych). Każde z takich urządzeń generuje przy swojej pracy pole elektromagnetyczne, które często jest niechcianym efektem ubocznym. W pewnych przypadkach takie promieniowanie może zawierać informacje o danych jakie przetwarza system, co stanowi potencjalne zagrożenie utraty ich poufności. Utrata niejawności informacji w zależności od rangi skompromitowanego systemu może nieść za sobą poważne konsekwencje, takie jak: straty majątkowe czy nawet zdrowie i ludzkie życie. Niniejsze opracowanie opisuje czym są emisje ujawniające oraz wskazuje czynniki jakie należy wziąć pod uwagę wyliczając bezpieczny poziom emisji dla systemów teleinformatycznych.

Słowa kluczowe: emisja ujawniająca, bezpieczeństwo informacji, cyberbezpieczeństwo

Abstract: Electronic devices belong to an indispensable component of present civilisation. They have been processing a wide spectrum of information (from entertainment, through medical and military data to important state matters). Each such operating device generates electromagnetic field which often is an unwanted side effect. In some cases such radiation can include information about data processed by a system what creates a potential risk of the loss of confidentiality. Depending on the rank of a compromised system the disclosed information can cause serious consequences, such as: losses of property, and even of health or human life. Presented paper describes the disclosing emissions and indicates the factors which have to be taken into account at calculation of a safe level of emission for tele-informative systems.

Keywords: disclosing emission, security of information, cybersecurity

1. Wstęp

Do pracy każdego urządzenia elektronicznego niezbędny jest przepływ prądu, który skutkuje emanacją pola elektromagnetyczne-

1. Introduction

A flow of electric current is needed for operation of each electric device and it produces emission of an electromagnetic field.

go. Emitowane przez różne urządzenia pola elektromagnetyczne mogą wzajemnie na siebie oddziaływać i w efekcie negatywnie wpływać na działanie systemów znajdujących się w pobliżu. Problematyka ograniczania poziomu niezamierzonych emisji jest określana mianem kompatybilności elektromagnetycznej. Głównym celem inżynierii kompatybilności elektromagnetycznej jest opracowanie metod pozwalających pracować urządzeniom w swoim bezpośrednim otoczeniu. Inżynieria kompatybilności elektromagnetycznej skupia się jednak tylko na poziomach emisji promieniowanej, nie biorąc pod uwagę źródła jej pochodzenia. Fakt ten nie likwiduje możliwości analizowania emisji o niskim poziomie w celu pozyskania z niej wartościowych informacji. W systemach teleinformatycznych przetwarzających informacje istnieje ryzyko, że niepożądana emisja elektromagnetyczna może zawierać w sobie elementy przetwarzanych danych. W związku z tym jest to emisja ujawniająca, która dodatkowo może dzielić się na emisje ujawniające przewodzone lub promieniowane, przy czym oba wymienione rodzaje dzielą się jeszcze na emisje pierwotne i wtórne.

Tabela 1W tabeli 1 przedstawiono uporządkowany podział typów emisji ujawniających.

Przypadki wykorzystania emisji promieniowanej do pozyskiwania informacji mają ponad 100-letnią historię. Jako jeden z pierwszych opisanych przypadków może służyć działanie niemieckiego wywiadu podczas I wojny światowej, gdzie podsłuchiwano łączność brytyjskiej armii w okopach. Brytyjskie telefony i telegrafy polowe wykorzystywały jeden rozciągnięty kabel oraz dobre uziemienie. Niemieckie urządzenia „Moritz" działały na zasadzie indukcji. Niemcy zagrzebywali w ziemi podłączone do kabla miedziane płytki, a drugi koniec przyłączali do „Moritza". Wzmacniacz urządzenia pozwalał na skuteczny

Electromagnetic fields emitted by different devices can interact mutually with each other, and in effect they can negatively affect the operation of systems in the vicinity. Questions relating to limitation of levels of unintended emissions are described as the electromagnetic compatibility. The electromagnetic compatibility engineering is mainly aimed at developing methods allowing the devices to work in their direct vicinity. But electromagnetic compatibility engineering is only focused on the levels of radiated energy without any consideration of its source of origin. And this does not prevent any possibilities for studying the low level emissions to recover valuable information. There is always a risk in tele-informative systems processing the information that unwanted electromagnetic emission may contain some parts of processed information. For that reason, it is a disclosing emission, which can be additionally divided into the conducted or radiated disclosing emissions, and both listed types are still divided into the primary and secondary emissions.

Table 1 shows the arranged division of disclosing types of emission.

Cases of using the emission of radiation for acquisition of information have been present in the history for more than 100 years. One of the first described cases took place during the 1-st world war by the German intelligence intercepting the communication of the British army in trenches. The British telephones and telegraphs used one wire and a good grounding. German devices named „Moritz" operated on the principle of induction. The Germans buried in the ground the copper plates which were connected by wires with „Moritz". The amplifier of the device enabled the efficient overhearing even at distances of 1000 m from the telephone line. The device was so effi-

podsłuch nawet z 1000 m od linii telefonicznej. Urządzenie było na tyle skuteczne i trudne do wykrycia, że dopiero w 1917 r. udało się Brytyjczykom wprowadzić w miarę skuteczne przeciwśrodki. Jednym z nich był zakaz prowadzenia rozmów telefonicznych w odległości mniejszej niż 3000 m od linii frontu.

cient and difficult for detection that only in 1917 the British side was able to introduce relatively effective countermeasures. And one of them concerned the ban of telephone communication at distances below 3000 m to the frontline.

Tabela 1. Podział emisji ujawniającej na podstawie mechanizmu przenoszenia informacji

MECHANIZM PRZENOSZENIA INFORMACJI		Rodzaj emisji	
		EMISJA PROMIENIOWANA	EMISJA PRZEWODZONA
TYP EMISJI	PIERWOTNA	Informacje przenoszone są na skutek niezamierzonej emisji fal elektromagnetycznych od elementów aktywnych urządzenia przetwarzającego te informacje.	Informacje przenoszone są na skutek przesłuchów poprzez elementy galwanicznie połączone do urządzenia przetwarzającego te dane.
	WTÓRNA	Informacje są przenoszone na skutek zjawiska wtórnej modulacji zewnętrznego pola elektromagnetycznego na przetwarzających informacje nieliniowych elementach danego urządzenia.	Informacja przenoszona poprzez element przewodzący, w którym została zaindukowana na skutek działania emisji promieniowanej od znajdującego się w pobliżu urządzenia przetwarzającego informacje.

Table 1. Division of disclosing emission on the base of information transfer mechanism

INFORMATION TRANSFER MECHANISM		Type of emission	
		RADIATED EMISSION	CONDUCTED EMISSION
TYPE OF EMISSION	PRIMARY	Information is transferred due to unintended emission of electromagnetic waves from active components of information processing device.	Information is transferred in effect of overhearing by galvanic components connected to data processing device.
	SECONDARY	Information is transferred due to the effect of a secondary modulation of the outer electromagnetic field on nonlinear components of information processing device.	Information is transferred via a conducting component which was induced in effect of action of a radiated emission originating from information processing device placed in vicinity.

Jak przedstawiono, elementami mogącymi być źródłem emisji ujawniającej nie są tylko i wyłącznie jednostki, które bezpośrednio te informacje przetwarzają. Do głównych źródeł emisji ujawniającej przewodzonej w systemach komputerowych zalicza się wszelkie interfejsy, do których podłączane są przewody (zarówno

As it was presented, the components which could be the sources of disclosing emission constitute not only and exclusively the units directly processing the information. The main sources of conducted emission in computerised systems are different types of interfaces with connecting wires (both signal and

sygnałowe jak i zasilające). Natomiast wtórnymi źródłami emisji mogą być nawet metalowe obudowy i ekrany.

W wielu krajach prowadzone są badania mające na celu opracowywanie i produkcje specjalistycznych urządzeń o ograniczonej emisji potocznie zwane TEMPEST. Nazwa pochodzi od uruchomionego w 1960 roku amerykańskiego programu rządowego (ang. Temporary Emanation and Spurious Trans-mission).

2. Możliwości wykorzystania emisji ujawniającej

Szczególnie podatnymi na zrekonstruowanie informacji na podstawie emisji ujawniającej mogą być wszelkiego rodzaju sygnały szeregowe, gdzie dane są przesyłane „bit po bicie" oraz sygnały okresowo powtarzalne, które dają możliwość uśredniania zmierzonych wyników, w celu eliminacji szumów otoczenia. Przykładami interfejsów, zawierających takie sygnały są: SATA, eSATA, FireWire itd.

W wyświetlaczach OLED (lub odmianach AMOLED itd.) obraz jest tworzony z pojedynczych punktów wyświetlanych przez odpowiednie fragmenty wyświetlacza, których wysterowanie odbywa się matrycowo.

W projektorach DLP za tworzenie obrazu odpowiada tysiące mikroluster, z których każde odpowiedzialne jest za tworzenie jednego piksela, kierując źródło światła w stronę obiektywu projektora lub w powierzchnię absorbującą światło. Za sterowanie tego typu rozwiązaniami odpowiadają chipy DMD (ang. Digital Micromirror Device).

W uproszczeniu sygnały sterujące wyświetlaniem obrazu odpowiadają za jego powstawanie punkt po punkcie, a następnie linia po linii (rys.1). Dodatkowo w wielu wyświetlaczach obraz odświeżany jest z równą i stałą częstotliwością 60 lub 120 Hz, co sprawia, że jest możliwe odebranie do 120 niewiele różniących się

supplying). And the secondary sources of emission may be even created by metallic cases and screens.

Many countries have been conducting research projects on development and production of specialised devices with limited emission commonly named by TEMPEST. The name originates from the US government program launched in 1960 (Temporary Emanation and Spurious Transmission).

2. Possibilities of Using the Disclosing Emission

All types of serial signals with the data transmitted "bit after bit" and the signals repeated periodically, which can be averaged to eliminate the environmental noises, are especially susceptible to reconstruction of information on the base of disclosing emission. Such signals are contained for instance in interfaces: SATA, eSATA, FireWire, etc.

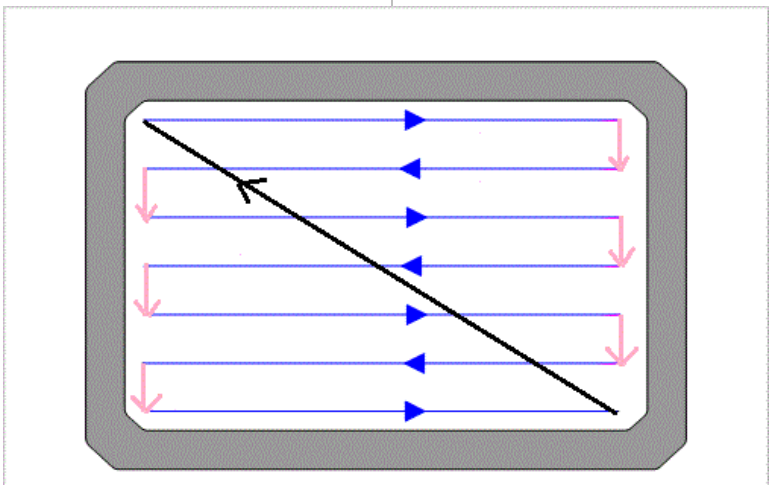
In displays OLED (or versions AMOLED etc.) the picture is created from individual points displayed by adequate fragments of the display which are controlled by a matrix.

Projectors DLP use thousands of micromirrors, and each of them is responsible for creation of one pixel directing the source of light towards the projector's optics or into the light absorbing surface. Such solutions are controlled by chips DMD (Digital Micromirror Device). In simplification, the signals controlling the displaying of picture are responsible for its creation point by point, and next line by line (Fig.1).

Additionally, in many displayers the picture is refreshed with an equal and permanent rate of 60 or 120 Hz, resulting in possibility for interception of up to 120 signals of spurious transmission with small

od siebie sygnałów emisji ujawniającej, co upraszcza ich agregacje i uśrednianie.

differences what facilitates their aggregation and averaging.

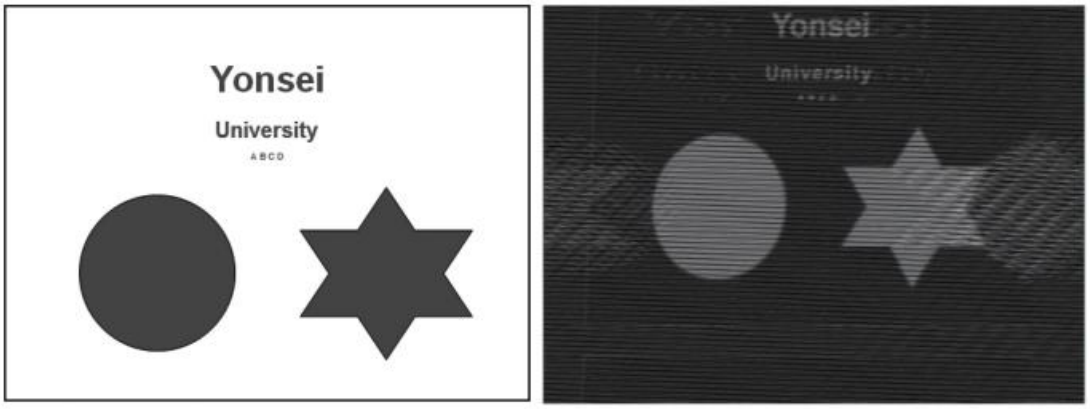


Rys. 1. Uproszczone zobrazowanie sekwencji powstawania obrazu w niektórych dostępnych technologiach

Fig. 1. Simplified illustration of a picture creating sequence in some accessible technologies

Panowie Ho Seong Lee, Dong Hoon Choi, Kyuhong Sim oraz Jong-Gwan Yook w pracy pt. „*Information Recovery Using Electromagnetic Emanations From Display Device Under Realistic Environment*" przedstawili ciekawe efekty przeprowadzonego przez siebie doświadczenia mającego na celu odtworzenie obrazu z monitora LCD laptopa na podstawie emisji ujawniającej. Co więcej, udało im się odtwarzać lekko zniekształcony obraz w czasie rzeczywistym.

Scientists Ho Seong Lee, Dong Hoon Choi, Kyuhong Sim and Jong-Gwan Yook presented in publication „*Information Recovery Using Electromagnetic Emanations From Display Device Under Realistic Environment*" some interesting effects of an experiment they carried out and which was aimed to reconstruct the image from laptop LCD monitor on the base of disclosing emission. And what's more, they were able to reconstruct slightly deformed image in the real time.



Rys. 2. Po lewej stronie obraz oryginalny, a po prawej odtworzony w czasie rzeczywistym

Fig. 2. Original image on the left side, and image reconstructed in real time on the right

Jednakże we współczesnych urządzeniach takie odtworzenie informacji może być utrudnione chociażby ze względu na to, że dane przesyłane poprzez przewód multimedialny mogą być szyfrowane. Na przykład popularny standard HDMI korzysta w tym celu z mechanizmu HDCP (ang. High-bandwidth Digital Content Protection). Oznacza to, że dopiero wewnątrz urządzenia obrazującego (np. monitora) występuje sygnał sterujący wyświetlaczem w postaci jawnej.

3. Kryteria oceny bezpieczeństwa systemów teleinformatycznych pod kątem emisji ujawniających oraz czynniki warunkujące ich podatność na infiltrację elektromagnetyczną

Różnorodność urządzeń, które mogą być potencjalnymi obiektami infiltracji elektromagnetycznej, jest na tyle duża, że nie sposób zebrać i opisać czynniki, które mogłyby pokryć sto procent przypadków. Uogólniając, można przyjąć, że w głównej mierze dopuszczalny, czyli bezpieczny poziom emisji ujawniającej od elementów przetwarzających informacje zależeć będzie przede wszystkim od:

- tłumienia otoczenia elementu przetwarzającego informacje,
- poziomu zakłóceń środowiskowych w miejscu instalacji elementu przetwarzającego informacje,
- zysku energetycznego wykorzystywanej metody odbioru i obróbki sygnału,
- czułości zestawu odbiorczego.

Zależność tę można opisać równaniem:

But such reconstruction of information can be difficult in present devices even because of the fact that the data sent via the multimedia wire can be coded. For instance, the popular standard HDMI employs for that reason the mechanism of HDCP (High-bandwidth Digital Content Protection). It means that only inside the imaging device (e.g. monitor) the signal controlling the display is in uncoded form.

3. Criteria Evaluating Security of Teleinformative Systems against Disclosing Emissions and Parameters of Their Susceptibility to Electromagnetic Infiltration

The variety of devices which may constitute potential objects of electromagnetic infiltration is so large that any collection and description of parameters covering one hundred percentage of cases is unrealistic. In general, it can be taken that the acceptable, i.e. safe, level of disclosing emission from components processing the information will depend most of all on:

- attenuation of the environment surrounding the component processing the information,
- the level of environmental interferences in the site where the component processing the information is installed,
- energetic gain of employed method of signal reception and processing,
- sensitivity of receiving system.

The dependence can be described by:

$$Us = \frac{U_N + U_R + A_P}{G_M} \tag{1}$$

lub wykorzystując miarę decybelową:

or using decibel measure:

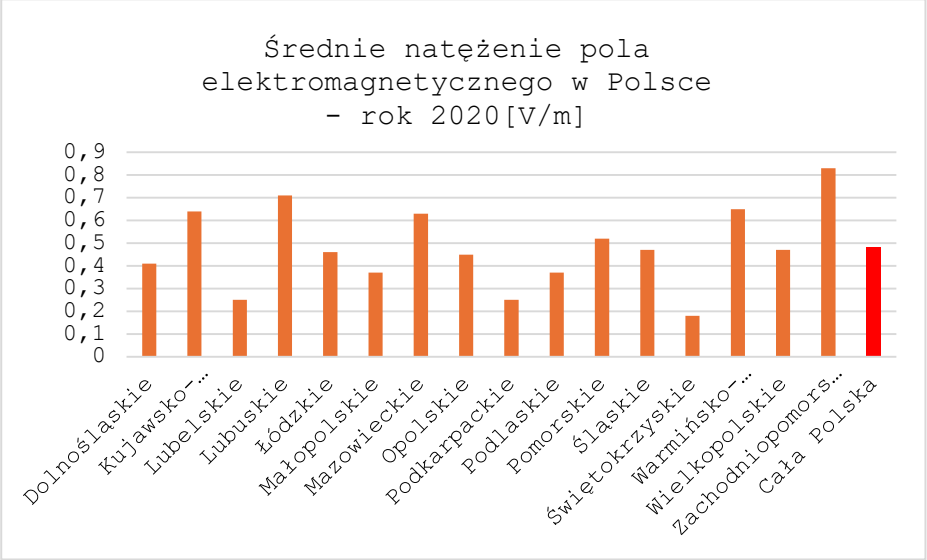
$$U_S = U_N + U_R + A_P - G_M \tag{1.1}$$

gdzie:
U_S – dopuszczalny poziom sygnału,
U_N – poziom zakłóceń otoczenia,
U_R – poziom szumów wprowadzanych przez zestaw odbiorczy,
A_P – tłumienie sygnału (przez otoczenie i elementy zestawu odbiorczego),
G_M – zysk energetyczny metody (wzmocnienie sygnału)

Z uwagi na różnorodność lokalizacji w jakich mogą pracować urządzenia przetwarzające informacje, w wymaganiach w zakresie dopuszczalnych poziomów emisji ujawniających należy wziąć pod uwagę minimalne poziomy zakłóceń środowiska w jakich urządzenie może występować (jest to tak zwana „metoda najgorszego przypadku"). Na rys. 5 przedstawiono średnie poziomy natężenia pola elektromagnetycznego w Polsce w roku 2020 opublikowane przez Główny Inspektorat Ochrony Środowiska.

where:
U_S – acceptable level of signal,
U_N – level of environmental interferences,
U_R – level of noise introduced by the receiver system,
A_P – attenuation of signal (by environment and components of receiving system),
G_M – energetic gain of the method (amplification of signal)

Because of the various localisations where the devices processing information can operate, in the requirements for acceptable levels of disclosing emissions the minimal levels of the environmental interference in which the device can operate (it is the so called "method of the worst case") have to be taken under the consideration. In Fig. 5 there are presented the average levels of the electromagnetic field intensity in Poland, in 2020, published by the Main Inspectorate of Environment Protection.



Rys. 3. Natężenie PEM w województwach w roku 2020 (źródło: GIOŚ)
Fig. 3. Intensity of electromagnetic radiation in 2020 *(source: GIOŚ)*

Należy dodać, że poziom zakłóceń środowiskowych nie jest zależny wyłącznie od lokalizacji, ale także od pory dnia, roku czy aktualnych warunków środowiskowych.

It has to be added that the level of environmental interferences is not exclusively dependant on the localisation, but also on the part of day, or year, or current environmental

Średnia arytmetyczna dla Polski to 0,48 V/m. Najniższe średnie natężenia pól występują na terenach wiejskich i są to wartości poniżej 0,3 V/m (czyli około 110 dBμV/m), więc taki poziom powinien być brany pod uwagę w ocenie bezpieczeństwa urządzeń na terenie naszego kraju jako wartość zakłóceń otoczenia w metodzie najgorszego przypadku.

Kolejnym czynnikiem warunkującym podatność utracenia poufności informacji jest szum termiczny odbiornika (spowodowany chaotycznym ruchem elektronów w ciałach stałych np. w strukturze półprzewodnikowej) oraz szum śrutowy powodowany przez fluktuacje prądu. Średniokwadratową wartość napięcia szumu termicznego odbiornika na impedancji wejściowej (zaciskach wejściowych) odbiornika pomiarowego opisuje wzór Johnsona-Nyquista:

conditions. The arithmetic mean for Poland is 0.48 V/m. The lowest mean intensities of fields are in the countryside and they are below 0.3 V/m (i.e. near 110 dBμV/m), and hence such level has to be taken in evaluation of security for devices in the territory of our country as the value of environment interferences in the method of the worst case.

Next parameter affecting the susceptibility of losing the confidentiality of information is the thermal noise of a receiver (caused by chaotic motions of electrons in solid bodies, e.g. in the structure of semiconductors) and the shot noise caused by the fluctuations of electric current. The mean squared value of thermal noise voltage on input impedance (input connectors) of a measurement receiver is described by Johnson-Nyquist's formula:

$$\bar{u}^2 = 4k_B \cdot T \cdot R \cdot \Delta f$$

Więc / *Hence*:

$$u_N = \sqrt{4k_B \cdot T \cdot R \cdot \Delta f} \tag{2}$$

gdzie:
$k_B - stała\ Boltzmanna = 1{,}38 \cdot 10^{-23}[J/°K]$
$T - temperatura\ [K]$
$R - rezystancja\ [\Omega]$
$\Delta f - pasmo\ częstotliwości\ szumu\ [Hz]$

where:
$k_B - Boltzman's\ const = 1.38 \cdot 10^{-23}[J/°K]$
$T - temperature\ [K]$
$R - resistance\ [\Omega]$
$\Delta f -$ noise frequency band $[Hz]$

Wartość skuteczną fluktuacji prądu opisuje wzór Schottky'ego (szum śrutowy):

The efficient value of electric current fluctuations is described by Schottky's formula (shot noise):

$$I_N = \sqrt{2 \cdot e \cdot I \cdot \Delta f}$$

Skąd / *Hence*:

$$u_N = R \cdot \sqrt{\frac{2 \cdot e \cdot u \cdot \Delta f}{R}} = \sqrt{2 \cdot e \cdot u \cdot R \cdot \Delta f} \tag{3}$$

gdzie:
$e - ładunek\ elementarny = 1{,}602176487(40) \cdot 10^{-19}[C]$
$I - średnia\ wartość\ prądu\ [A]$
$\Delta f - pasmo\ częstotliwości\ szumu\ [Hz]$
$u - średnia\ wartość\ napięcia\ [V]$
$R - rezystancja\ [\Omega]$

where:
e –elementary charge $= 1{,}602176487(40) \cdot 10^{-19}[C]$
$I -$ mean value of current $[A]$
$\Delta f -$ noise frequency band $[Hz]$
$u -$ mean value of voltage $[V]$
$R - resistance\ [\Omega]$

Na podstawie powyższych wzorów można wyliczyć minimalne wartości szumów termicznego i śrutowego:

The above formulae can be used to calculate the minimal values of thermal and shot noise:

$$u_{N_{min}} \approx -7dB\mu V$$
$$u_{SN_{min}} \approx -50dB\mu V$$

$u_{N_{min}}$ – minimalny poziom napięcia szumów na wejściu odbiornika pomiarowego w temperaturze pokojowej, przy wejściu zwartym impedancją wejściową = 50Ω, dla pasma analizy BW=1MHz.

$u_{SN_{min}}$ – minimalny poziom napięcia szumów śrutowych na wejściu odbiornika pomiarowego w temperaturze pokojowej, przy wejściu zwartym impedancją wejściową = 50Ω, dla pasma analizy BW=1MHz.

$u_{N_{min}}$ – minimal level of noise voltage on the input of a measurement receiver at ambient temperature and at input termination impedance of = 50Ω, for the analysed bandwidth BW=1MHz.

$u_{SN_{min}}$ – minimal level of shot-noise voltage on the input of a measurement receiver at ambient temperature and at input termination impedance of = 50Ω, for the analysed bandwidth BW=1MHz

Należy zauważyć, że w rzeczywistym systemie odbiorczym wystąpią jeszcze szumy wprowadzane przez elementy aktywne takie jak anteny odbiorcze (zamiast zwarcia o impedancji 50Ω). Aby wyliczyć szumy wprowadzane przez cały układ odbiorczy należy uwzględnić szumy wprowadzane przez poszczególne jego elementy. W praktyce najlepiej do takich wyliczeń posłużyć się parametrami *Noise Factor* i *Noise Figure* poszczególnych elementów aktywnych.

It has to be noted that in the real receiving system there are still present noises introduced by active components such as receiving antennas (instead termination with 50Ω impedance). The noises introduced by the overall receiving system can be calculated by counting the noises introduced by its particular components. In practice, such calculations can be assisted by parameters of *Noise Factor* and *Noise Figure* for particular active components.

$$F = \frac{SNR_{IN}}{SNR_{OUT}} \tag{4}$$

gdzie / *where*:

F – parametr Noise Factor danego elementu
F – *parameter Noise Factor for particular component*
SNR_{IN} – stosunek poziomu syg. użyt. do poziomu szumu na wej. elementu
SNR_{IN} – *ratio of the useful signal level to the noise level in the input of component*
$\mathrm{SNR_{out}}$ – stosunek poziomu syg. użyt. poziomu szumu na wyj. elementu
$\mathrm{SNR_{out}}$ – *ratio of the useful signal level to the noise level in the output of component*

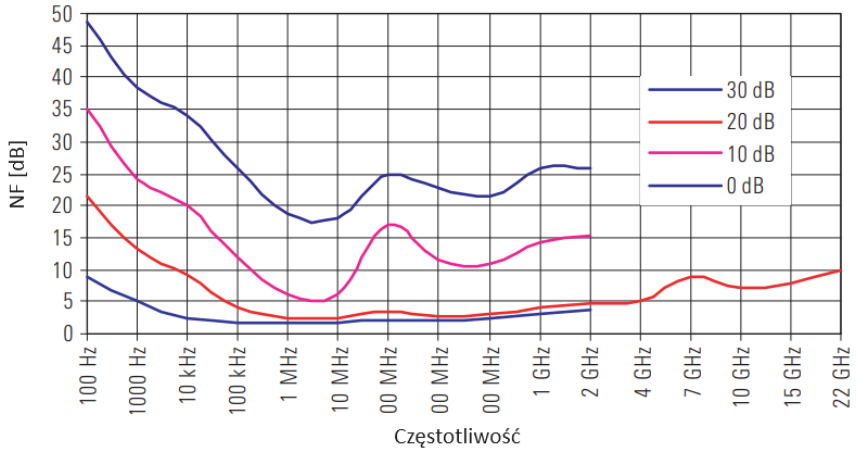
$$NF = 10 \cdot \log(F) = 10 \cdot \log(\frac{SNR_{IN}}{SNR_{OUT}}) \tag{5}$$

gdzie /where:

NF – parametr Noise Figure danego elementu / *parameter Noise Figure of component*

W przypadku elementów biernych (bez wzmocnienia) przyjmuje się, że *Noise Figure* jest równy tłumieniu L wprowadzanemu przez nie do obwodu. Biorąc pod uwagę powyższe czynniki, można stwierdzić, że możliwe jest skonstruowanie systemu odbiorczo badawczego, którego parametr NF nie jest większy niż 5-10 dB (np. układ składający się z odbiornika Rohde&Schwarz FSET z niskoszumowym układem antenowym R&S AM-524). Należy również zauważyć, że parametry NF i F całego systemu są zależne od częstotliwości oraz temperatury (poziom szumów na wejściu i wyjściu badanego elementu zwiększa się wraz z jej wzrostem).

In the case of passive components (without amplification) it is accepted that *Noise Figure* equals to attenuation L introduced by them into the circuit. Considering the above mentioned parameters it can be stated that it is possible to design a receiving-testing system having the parameter of NF below 5-10 dB (for instance a system containing receiver Rohde&Schwarz FSET with low noise antenna unit R&S AM-524). It has to be also noted that parameter NF and F of the whole system depend on frequency and temperature (level of noises in the input and output of tested device increases along with temperature).



Rys. 4. Uśredniona zależność parametru NF od częstotliwości dla układów odbiorczych R&S FSET7, R&S FSET22 z preselektorami RF R&S FSET-Z2, R&S FSET-Z22 dla różnych wartości wzmocnienia sygnału

Fig. 4. Averaged dependence of parameter NF on the frequency for receivers R&S FSET7, R&S FSET22 with preselectors RF R&S FSET-Z2, R&S FSET-Z22 for different values of signal amplification

Tłumienie sygnału przez otoczenie to kolejny z czynników, który należy wziąć pod uwagę w ocenie możliwości odbioru emisji ujawniających. Tłumienie w wolnej przestrzeni (ang. Free Space Loss) w strefie dalekiej wynosi:

Attenuation of the signal in the environment is a next parameter to be considered at evaluation of possibilities for reception of disclosing emissions. The free space loss in the far zone is:

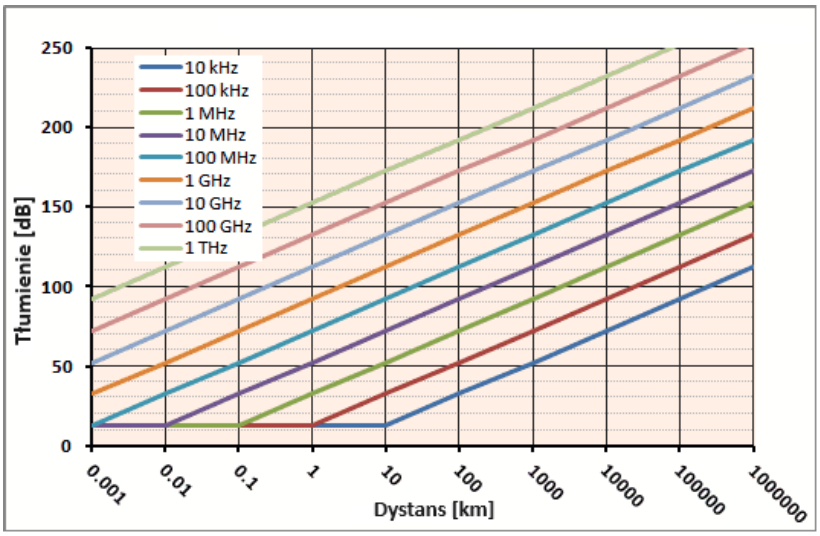
$$FSL = 20 \cdot \log(f) + 20 \cdot \log(d) - 27{,}6\ [dB] \tag{6}$$

Często, jako granicę strefy bliskiej i dalekiej przyjmuje się (w uproszczeniu) odle-

The limit separating the close and far zones is often taken (in simplification) at the

głość λ/2π. W praktyce podawanie powyższego parametru nie ma zastosowania, gdyż w większości przypadków pomiary urządzeń z zakresu kompatybilności elektromagnetycznej wykonuje się w ustandaryzowanej odległości 3 lub 10 m. Dla urządzeń o obniżonej emisyjności ta odległość może być jednak zmniejszona do 1 metra.

distance of λ/2π. In practice the above parameter is meaningless as in the most cases the measurements of devices over the electromagnetic compatibility are performed at standardised distances of 3 or 10 m. But for the devices with reduced emissivity this distance may be limited to 1 meter.



Rys. 5. Teoretyczne tłumienie sygnałów w wolnej przestrzeni o różnej częstotliwości w zależności od odległości [7]

Fig. 5. Theoretical attenuation of signals in the free space for different frequencies depending on distance [7]

Niezwykle istotne jest określenie granicy pomiędzy strefą bliską, a daleką, ponieważ jedynie w strefie dalekiej można z dużą dokładnością szacować tłumienie wnoszone przez otoczenie systemu przetwarzającego informacje. Zgodnie z przedstawionym wyżej wzorem jest to 20 dB na dekadę przyrostu odległości. Uwzględniając standardowy sposób instalacji urządzeń teleinformatycznych, a także zasadę najgorszego przypadku, można stwierdzić, że minimalne wypadkowe tłumienie wolnej przestrzeni dla urządzeń służących do przetwarzania informacji należy oszacować dla odległości nie większej niż 2 metry (zgodnie z zasadą najgorszego przypadku należy uwzględnić odległość do granicy strefy pod i nad miejscem instalacji urzą-

Establishing a borderline between the close and far zones is highly significant because the attenuation caused by the environment of the system processing the information can be estimated with a high accuracy only in the far zone. According with the formula presented above it is 20 dB for each decade of distance increment. Considering a standard method of installation of tele-informative devices, and also the principle of the worst case, it can be stated that the minimal resultant attenuation of the free space for devices used for processing of information has to be estimated for a distance which is not larger than 2 meters (according with the principle of the worst case a distance to the border of the zone below and over the site where the information processing

dzenia przetwarzającego informacje z uwzględnieniem grubości stropów i minimalnej odległości instalacji potencjalnego systemu antenowego). Standardowo systemy IT instalowane są najczęściej w tradycyjnych pomieszczeniach biurowych (za ścianami, stropami itd.), a wprowadzenie do strefy bezpieczeństwa dodatkowej tłumienności można traktować jako równoważne rozszerzeniu tej strefy proporcjonalnie do wprowadzonej tłumienności. Współczynnik Rozszerzenia Strefy (WRS) można wyliczyć ze wzoru:

device is installed has to be taken into account together with the thickness of floors and minimal distance of installation of a potential antenna system). In standard cases the IT systems are most often installed in traditional office rooms (behind the walls and floors, etc.) and any introduction of an additional attenuation into the security zone can be treated as an equivalent extension of this zone, proportionally to the introduced attenuation. The Coefficient of Zone Extension (CZE) can be calculated with formula:

$$WRS_{AD} = 10^{(AD/20)} \tag{7}$$

gdzie:
$AD -$ tłumienność dodatkowa [dB]
kalkulacyjny promień takiej strefy bezpieczeństwa emisji wynosi:

where:
$AD -$ additional attenuation [dB]
Calculative radius of such zone of security is:

$$KR_{R:AD} = WRS_{AD} \cdot \mathrm{R} \tag{8}$$

gdzie:
$R -$ promień strefy bezpieczeństwa emisji $[m]$

where:
$R -$ radius of security zone for emission $[m]$

I tak np. umieszczenie urządzenia w pomieszczeniu o ścianach z cegły silikatowej, które charakteryzują się tłumiennością 4 dB przy równoczesnym zapewnieniu wokół strefy o promieniu R = 2 m, z punktu widzenia poziomu sygnału na granicy strefy bezpieczeństwa, będzie równoznaczne z umieszczeniem urządzenia w wolnej przestrzeni w strefie bezpieczeństwa emisji o promieniu KR = 3 m (jest to kalkulacyjny promień strefy bezpieczeństwa), gdyż:

And for instance, locating the device in a room with walls made of silicate bricks having the attenuation of 4 dB and providing at the same time the surrounding zone with radius of R = 2 m, will be equivalent of placing the device in a free space in the zone of safe emission with the radius of KR = 3 m, regarding the point of view of the signal level on the border of the security zone (it is a calculative radius of the security zone), because:

$$RS_{4dB} = 10^{(4/20)} \approx 1{,}6 \;\rightarrow\; KR_{2:4dB} = WRS_{4dB} \cdot 2 \approx 3\,m \tag{9}$$

W tabeli 2 zamieszczono szacunkowe wartości tłumienności wybranych przegród budowalnych dla sygnałów o częstotliwości 2,4 GHz, czyli częstotliwości na jakiej pracuje np. popularny standard Wi-Fi.

Table 2 presents the estimated values of attenuations for selected construction walls and signals with frequency of 2.4 GHz used by popular standard Wi-Fi.

Considering these data, some trials can

Mając na uwadze te dane można próbować szacować różne teoretyczne scenariusze tłumienności różnych stref bezpieczeństwa.

be made to estimate different theoretical scenarios of attenuation for various zones of security.

Tabela 2. Orientacyjna tłumienność przykładowych przegród budowlanych
Table 2. Estimated attenuation of some exemplary construction walls

Rodzaj przegrody ***Type of wall***	**Materiał** ***Material***	**Grubość [cm]** ***Thickness***	**Tłumienność [dB]** ***Attenuation***
Ściana działowa *Partition wall*	Cegła *Bricks*	10	~7
Ściana nośna *Bearing wall*	Cegła *Bricks*	30	~9
Ściana działowa *Partition wall*	Płyta gipsowa i wełna szklana *Plaster plate and glass wool*	7	~2
Strop *Roof*	beton zbrojony *Reinforced concrete*	30	~11
Okna *Windows*	Szkło *Glass*	2 x szyba + 1 cm przerwa pomiędzy *Double glazing with 1 cm gap*	~4,5
Drzwi *Doors*	Drewno *Wood*	4	~2,5

Tabela 3. Scenariusze tłumienności dla teoretycznych stref bezpieczeństwa

Typ strefy bezpieczeństwa	**Opis**	**R_{MIN}[m]**	**KR[m]**
Bardzo mała	System zlokalizowany w małej firmie – minimalny rozmiar strefy bezpieczeństwa	2	3
Średnia	System zlokalizowany w małej strefie bezpieczeństwa (brak pełnej kontroli nad terenem wokół budynku) – typowy system w małej lub średniej firmie np. w wynajmowanym budynku.	5	8
Duża	System zlokalizowany w budynku oddalonym o 15-20 m od ogrodzenia stanowiącego granice strefy bezpieczeństwa	15	20

Table 3. Scenarios of attenuation for theoretical security zones

Type of security zone	**Description**	**R_{MIN}[m]**	**KR[m]**
Very small	System localised in a small company – minimal size of the security zone	2	3
Medium	System localised in a small security zone (lack of complete control over the area near building) – typical system in a small or medium company for instance in a hired building	5	8
Large	System localised in a building 15-20 m away from a fence constituting the limits of the security zone	15	20

W praktyce dokładne określenie tłumienności danej strefy bezpieczeństwa wymagałoby przeprowadzenia badań empirycznych.

Dodatkowym czynnikiem utrudniającym odbiór emisji ujawniających w standardowym środowisku pracy mogą być silne sygnały radiowe (np. od nadajników radiowych czy telewizyjnych) oraz inne zakłócenia środowiskowe (np. naturalne wyładowania elektryczne).

Metodą ograniczania wpływu takich zakłóceń może być akwizycja emisji ujawniających równocześnie na kilku częstotliwościach lub w różnym czasie. Po cyfrowym przetworzeniu takich próbek istnieje teoretyczna możliwość pozbycia się wcześniej wspomnianych sygnałów zakłócających.

Kolejną metodą eliminacji niechcianych sygnałów zakłócających może być wykorzystanie zasady odbioru zbiorczego - rejestracji sygnałów z kilku anten jednocześnie, przy czym przynajmniej jedna z nich powinna znajdować się w pobliżu źródła emisji ujawniającej, zaś pozostałe z dala od niego. Odwracając w fazie sygnały zakłóceń środowiskowych (zebrane antenami znajdującymi się z dala od źródła interesującej nas emisji) oraz sumując je z sygnałami zawierającymi emisje użyteczną (zebraną poprzez antenę blisko źródła) można niwelować większość zakłóceń natury środowiskowej.

Szczególnie podatnymi na infiltracje elektromagnetyczną są transmisje szeregowe i dodatkowo powtarzalne (np. w monitorach, gdzie klatki obrazu nie różnią się znacząco między kolejno sąsiadującymi). Poprzez uśrednianie bardzo podobnych do siebie sygnałów można znacząco poprawić wartość parametru SNR (ang. Signal Noise Ratio) odebranego sygnału. Zysk ten można opisać następującą zależnością:

In practice, the accurate identification of attenuation of a specific security zone would require empirical tests to be carried out.

Strong radiobroadcast signals (for instance radio or TV transmitters) and other environmental interferences (for instance natural electric discharges) can be an additional factor harming the reception of disclosing emissions in the standard environment of work.

A method limiting the influence of such interferences can be based on the acquisition of disclosing emissions on a few frequencies in the same time or in different times. After digital processing of such samples there is a theoretical chance for removal of interfering signals which were mentioned earlier.

A next method eliminating the unwanted interfering signals can be based on the principle of aggregated reception - recording the signals from a few antennas at the same time whereas at least one of them has to be placed in the vicinity of the source of disclosing emission and the others have to be placed away of it. Reversing the phase of environmental interferences (picked up by antennas placed away from the source of interesting emission) and summing it with the signals containing the useful emission (picked up by antenna placed close to the source) can neutralise most of the interferences of environmental character

The serial and repeatable transmissions (for instance in monitors where the consecutive frames of image are similar to each other) are especially susceptible to electromagnetic infiltration. The averaging of signals which are very similar to each other can significantly improve the value of parameter SNR (Signal Noise Ratio) for received signal. The gain can be described by expression:

$$G = SNR_U - SNR_P = 10 \cdot \log(\mathrm{N})^{39} \tag{10}$$

gdzie:

$SNR_U = 10 \cdot \log\left(\frac{S_U}{N_U}\right) - stosunek\ mocy$
$sygnału\ do\ mocy\ szumu\ po\ uśrednieniu;$
$SNR_P = 10 \cdot \log\left(\frac{S_P}{N_P}\right)$
$SNR_P - początkowy\ stosunek\ mocy$
$sygnału\ do\ mocy\ szumu.$
$S_U - poziom\ sygnału\ po\ uśrednieniu$
$N_U - poziom\ szumu\ po\ uśrednieniu$
$N -$ ilość uśrednionych sygnałów.

4. Podsumowanie

Biorąc pod uwagę informacje przedstawione w poprzednich rozdziałach, można stwierdzić że emisja ujawniająca od urządzeń teleinformatycznych stanowi realne zagrożenie, które należy brać pod uwagę podczas projektowania urządzeń oraz stref bezpieczeństwa, w których dany system może pracować. Emisje od urządzeń przetwarzających dane szeregowo „bit po bicie" stanowią najmniejsze wyzwanie w odtworzeniu tychże danych na podstawie pomiaru emisji ujawniającej, a szczególnie niebezpieczne są dodatkowo wszelkie emisje o charakterze powtarzalnym (np. od monitorów, których częstotliwość odświeżania to kilkadziesiąt Hz). Wiele urządzeń obrazujących dane pracuje obecnie w oparciu o procesory obrazowe typu RIP (ang. Raster Image Processor). Tworzą one obraz w sposób szeregowy i powtarzalny w związku z tym mogą być potencjalnie niebezpieczne.

Aby określić jasne wymagania warunkujące bezpieczną eksploatacje urządzeń teleinformatycznych, zgodnie z informacjami zawartymi w poprzednich rozdziałach poziom dopuszczalny emisji promieniowanych można wyliczyć dla konkretnego przypadku według zależności:

where:

$SNR_U = 10 \cdot \log\left(\frac{S_U}{N_U}\right) -$ ratio of signal power
$to\ power\ of\ noise\ after\ averaging;$
$SNR_P = 10 \cdot \log\left(\frac{S_P}{N_P}\right)$
SNR_P – original ratio of signal power
to noise power;
$S_U - level\ of\ signal\ after\ averaging;$
$N_U -$ level of noise after averaging ;
$N -$ number of aweraged signals .

4. Summary

Regarding the information presented in former chapters one can note that the disclosing emission from tele-informative devices creates a real threat which has to be considered during designing process of devices and security zones in which the system can operate. Emissions from devices with a bit-by-bit series data processing constitute the lowest challenge in reconstruction of the data on the base of disclosing emission measurements, and additionally all emissions of a repeatable character (e.g. from monitors with the rate of refreshing equal to a few dozens of Hz) are especially dangerous. Many devices for data imaging operate now on the base of imaging processors RIP (Raster Image Processor). They create the image using a series and repeatable method and therefore they can be potentially dangerous.

To establish clear requirements for conditions of the safe use of tele-informative devices in accordance with the information contained in previous chapters the acceptable level of radiated emissions can be calculated for a specific case with the dependence:

$$U_{S[RMS]} = U_N + U_R + A_P - G_M[\frac{dB\mu V}{m}] \quad (11)$$

$U_N - poziom\ szumów\ otoczenia\ \left(zgodnie\ z\ rys.3 - dane\ przekształcić\ na\ \frac{dB\mu V}{m}\right)$

$U_N -$ level of ambient noise $\left(according\ to\ Fig.3 - data\ expressed\ in\ \frac{dB\mu V}{m}\right)$;

$U_R - poziom\ szumów\ NF\ wprowadzony\ przez\ konkretny\ zestaw\ odbiorczy.$
$Prawdopodobnie\ wartości\ pomiędzy\ 5-10\ dB\ (przykładowo\ rys.4);$
$U_R -$ noise level $NF\ introduced\ by\ a\ specific\ receiver.$
$Probable\ values\ between\ 5-10\ dB\ (example\ in\ Fig.4).$

$A_P - tłumienie\ sygnału$ (zgodnie z informacjami przedstawionymi na rys. 5 i w tabeli 2).
$A_P -$ signal attenuation (according to information presented in Fig.5 and table 2);

$G_M -$ zysk energetyczny metody (wzmocnienie sygnału) wynikający z aparatury odbiorczej i metod obróbki sygnału. Zgodnie z informacjami zamieszczonymi w poprzednim rozdziale);
$G_M -$ energetic gain of the method (amplification of signal) resulting from the receiver and methods of signal processing. According to information contained in previous chapter).

Bibliografia / *Bibliography*

[1] Lee HS, Choi DH, Sim K, Yook JG (2019) *Information Recovery Using Electromagnetic Emanations from Display Devices under Realistic Environment*. IEEE Transactions on Electromagnetic Compatibility. Aug;61(4):1098-1106. 8423652. doi: 10.1109/TEMC.2018.2855448.

[2] Więckowski T.W., Pomiar emisyjności urządzeń elektrycznych i elektronicznych, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 1997.

[3] Szczepankiewicz K, Wnuk M, (2023) *Embedded Systems and their Vulnerabilities to Hardware Attacks,* Bulletin of the Military University of Technology.

[4] Fan Zhang, Wang Wang, Dongrong Zhang, Aixin Chen, Donglin Su (2022) *Radiation Emitter Classification and Identification Approach Based on Radiation Emission Components*, artykuł opublikowano w otwartym dostępie na stronie https://www.mdpi.com/2076-3417/12/16/8193, 2022.

[5] K. Grzesiak, I. Kubiak, S. Musial and A. Przybysz (2012), *Elektromagnetyczne bezpieczenstwo informacji*, Wydawca:WAT, Zegrze.

[6] Mordechai Guri (2022) *SATAn: Air-Gap Exfiltration Attack via Radio Signals From SATA Cables*, 19th Annual International Conference on Privacy, Security & Trust (PST), pp.1-10.

[7] Wykres z artykułu *Free Space Path Loss Friis Equation Formula* - RF Cafe pobrany z https://www.rfcafe.com/

[8] M.A. Azpúrua, M. Pous and F. Silva (2015) *A measurement system for radiated transient electromagnetic interference based on general purpose instruments*", Electromagnetic Compatibility (EMC EUROPE) International Symposium on Electromagnetic Compatiblity.

[9] F. Alessandro, P. Dario, C. Paolo and M. Catelani (2015) EMC measurements in Modern Measurements: Fundamentals and Applications, Wiley-IEEE Press, vol. 1, no. 400.

[10] W. Diehl M. Randolph (2020) *Power Side-Channel Attack Analysis: A Review of 20 Years of Study for the Layman*. Blacksburg: The Bradley Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University.

[11] P. C. Kocher (1996) *Timing Attacks on Implementations of Diffie-Hellman*. Berlin: Springer.

[12] Awan F. G., Sheikh N. M., Qureshi S. A., Ali A. (2008) *A Generic Model for the Classification of Radiation Emission Data in Electromagnetic Compatibility Measurement*, Radio and Wireless Symposium, 2008, ISBN: 978-1-4244-1462-8.

[13] Han Fang, Shi Changsheng, Deyun Lin, Guoding Li (1991) *Measurement of radiated emission from PC computer system*, CH3044-5/91/0000-0208 $01 .OO 0 IEEE.

[14] Vuagnoux M. Pasini S. (2010) *An improved technique to discover compromising electromagnetic emanations*, Electromagnetic Compatibility (EMC) IEEE International Symposium on Digital Object Identifier.