IJCTA, 9(30), 2016, pp. 09-19

Detection of Informative Components of Compromising Electromagnetic Emanations of Computer Hardware

Anton Borisovich Tokarev* Vladimir Mikhailovich Pitolin* Svetlana Yurievna Beletskaya* and Alexander Vasilyevich Bulgakov*

Abstract : This article discusses the problem of detection of technical channels of information leakage caused by compromising electromagnetic emanations (CEME) of computer aids. From the point of view of data protection not all but only informative components of CEME can pose threat. Conventional approach, which assumes searching for all CEME components with their subsequent sub dividing into informative and non-informative, can be applied but it is extensive. This work proposes an alternative algorithm of panoramic search of CEME informative components in wide frequency range based on development of on-line software controlled change of operation mode of tested equipment units. It is demonstrated that probability of detection of informative CEME on the basis of the proposed algorithm is at least the same as that of conventional approach on the basis of consecutive narrow-band filtering into combinations of potentially hazardous frequencies, however, the panoramic search enables significant reduction of testing by means of superposition of detection and testing phases of CEME component informativity. Recommendations are given concerning selection of thresholds of detection and optimization of processing parameters. Results of experimental verification of the proposed algorithm are given for the case study of detection of informative CEME components accompanying video data displayed on PC monitor.

Keywords : Radio monitoring, compromising electromagnetic emanations, detection of informative components, techniques of information leakage, interception of information.

1. INTRODUCTION

1.1. Reasons of occurrence of compromising electromagnetic emanations (CEME)

Operation of any radio engineering devices is in separably associated with occurrence of electromagnetic fields (EMF) in their environment. For some devices emanation of electromagnetic waves is the main task, for other devices occurrence of EMF is compromising and, rather often, undesirable consequence of their operation. Electro magnetic waves generated in environment by devices, that are not designed to emit radio waves, are known as compromising electromagnetic emanations (CEME). Properties of CEME, generated by computer hardware(CHW) units, are interrelated with processed data, and hence, while analyzing the pattern of variations of these emanations by means of sensitive intelligence receiver, the processed CHWdata could be restored. In order to prevent information leakage the intensity of informative CEME components of CHW units should be monitored, which in its turn leads to necessity of development of algorithms of their detection.

* Voronezh State Technical University, Moskovskii prospekt, 14 Voronezh 394026 Russia.

1.2. Researches in the field of detection and interception of CEMEand their importance

Arrangement of information interception via CEME channel and protection against such interception is very peculiar field of radio engineering. CEME have moderate intensity and are emanated into environment by means of "random" antennas in the form of some cables and CHW units, hence, even dedicated equipment and possibility of location of such equipment at the distance of tens (or even units) of meters from emanating CHW do not guarantee successful interception of CEME. However, in rare cases when random factors produce operating channel of information leakage, the hazard of CEME phenomenon is extremely high due to its in visibility for CHW owners, because receiving of information by an enemy does not influence on CHW, and detection of leakage possibility can be established only by rather labor consuming high-skilled investigation supported by dedicated soft- and hardware. In this regard, starting from open access publication by*VanEck (1985)*, the experts in the field of interception and protection of information pay great attention to the research scope of CEME.

The article by *Kuhn* (*2003*) is one of the framework open access publications, which, in addition to equipment and procedures of interception of information displayed in PC monitors, provides expert estimation of noise intensity, against which the CEME components are to be detected. The procedure of calculation and measurement of intensity of electromagnetic fields, generated by CEME, as well as recommendations on calculation of security zone of CHW with regard of information leakage via CEMEchannel can be found elsewhere: *Sudarikov and Romashchenko* (*2011*), *Lykov and Syagaeva* (*2012*), *Korolev* (*2013*), *Zidong and Yuanhui* (*2014*). Data required for calculation of CEME attenuation on objects of computerization can be found in *Asotov, SIBCON-2015 and Asotov, CriMiCo-2015*. Some studies are devoted to detailed description of the mechanism of attack and data interception. In addition to the mentioned work by *Kuhn* (*2003*), data interception is discussed in *Kuhn and Anderson*(*1998*), *Horev*(*2014*) and many others. Peculiar attention in numerous recent works is paid to interception of keyboard information (*Vuagnoux and Pasini, 2009*; *Vuagnoux and Pasini, 2010*; *Dmitryievetal., 2013*; *Ahsanetal., 2014*; *Sokolov, 2016*). Obvious interest is given to specialized researches concerning, for instance, analysis of reasons of occurrence and features of CEME interception, accompanying operation of printers (*Przesmycki, 2014*), or data transfer by USB2 interface (*Nowosielski and Wnuk, 2014*), and others (*Rohatgi, 2009*).

In addition to the studies directed at detailed description of CEME properties, generated by specific CHW units, there are some interesting works considering the phenomenon of CEME occurrence and information protection procedures in total (*Ivanov, 2007*; *Ermakova and Shlegel, 2008*; *Gorobets and Trivaylo, 2009*; *Poyarkov et al., 2012*; *Meynardetal., 2012*; *Filin et al., 2013*; *Anishchenko et al., 2014*). Separate group of works is devoted to development and description of searching complexes intended for CEME analysis, as well as detailed description of execution of specialized studies aimed at estimation of information security with regard to information leakage via CEME channel (*Buzov et al., 2005*; *Tupota et al., 2006*; *Horev, 2007*; *Cazanaru et al., 2011*; *Frankland, 2011*; *Filippovich, 2014*;*Ulas et al.,2014*).

However, despite the mentioned variety of works, the CEME detection is mostly "manual" operation and the procedure of search automation is still uncertain. Procedures of detection of informative CEME components presented in open access publications (*Bekhtin, 2009*; Soft- and hardware complex for searching of adverse electromagnetic emanations: "Navigator", Comparative analysis of methods) are poorly described and rather labor consuming, that is, the study of alternative procedures of search automation of informative CEME components is rather urgent.

1.3. Typical procedure of detection of informative CEME components

Typical procedure of detection of informative CEME componentsis comprised of two stages (*Radio Monitoring,* 2009).

The first stage is based on comparison of averaged periodograms, calculated for all monitored frequency range. At first, the observed spectral estimations are averaged in passive mode of tested equipment. Then, spectral data are acquired again by toggling the tested equipment into test mode, where signals of CHW unit are presented by periodic sequences of bursts, which provides concentration of signal power in narrow frequency bands. By means of comparison of accumulated spectral periodograms it is possible to detect the set of frequencies of CEME components to be tested for informativity. Here with, in order to avoid omitting of weak CEME components at the first stage upon comparison of periodograms even small deviations of intensities (units of decibels) are considered as significant, and the list of frequencies to be tested becomes very long.

The second stage is aimed at testing of informativity of all "suspicious" frequencies. This testing is carried out by successive narrow band processing of CEME components included in the list. Informativity criterion is comprised of detection of interrelation between operation mode of tested equipment and observed frequency distribution of power of spectral components. The tradition of the use of narrow band processing is dated to the time of informativity testing by operator aurally: by variation of tonality of demodulated signal occurring simultaneously with toggling of tested equipment into new operation mode.

It should be noted, however, that upon adequate efforts by developers of radio monitoring complexes the operation mode of tested CHW units can be often controlled by monitoring complex. If, in addition, the radio monitoring equipment is able to analyze properties of radio emanations in wide frequency range with high spectral resolution (at least some hundred of Hertz), then it becomes possible to develop and implement into practice an alternative algorithm of detection of informative CEME components, which provides combination of searching and testing of informativity of detected CEME components in one procedure. Exactly this combined processing algorithm will be discussed below.

2. METHOD

2.1. Features of data acquisition procedure

The analyzed in this work method of automated searching for informative CEME components is oriented at its application in wide band systems of radio monitoring similar to those described in (*Radio Monitoring*, 2009). Such systems analyze radio environment in wide frequency ranges by means of their panoramic review. The analyzed range is subdivided into bands with the widths determined by possibilities of radio monitoring receivers and equaled usually from units to tens of megahertz. The receiver consecutively retunes from one band to another and, after completion of transient processes, records complex data samples. The size of the data samples is chosen in accordance with the solved radio engineering problem. Upon rapid wide band analysis of radio environment the duration of data acquisition can be equal to some milliseconds, and in the case of other tasks it can be significantly higher. Due to usage such short data samples and circuit optimization aimed to minimize time loss for frequency retuning, modern radio monitoring systems can provide the rate of radio environment analysis of higher than 1 GHz per second.

Another mandatory feature of data acquisition procedure is the use of online programmable toggling of operation mode of tested CHW unit. The state of tested unit, corresponding to minimum possible level of compromising emanations, will be referred to as **passive**. In the case of analogous monitor the passive mode corresponds to dark screen, for keyboard: no pressing at all. The alternative state is **active** or **test** state of the considered unit, when formation of CEME with the highest possible level is assumed. The mentioned state is implemented by means of maximum frequent periodic change of information signal. In the case of anaogous monitor the active mode corresponds to displayed sequence of black and white vertical lines; for keyboard: emulation of automated pressing of any key with maximum rate.

Periodicity of signals, formed in test operation mode, generates radio emanations, the spectrum of which is linear (Fig. 1). Hence, detection of CEME components should be reasonably performed in spectral region. With this aim the time domain data samples of the observed signals $s_{(r)}(k)$, where r is the number of the set of samples, k is the serial number of sample in the current set ($0 \le k \le \mathrm{N}-1$, N is the number of data sets), recorded by radio monitoring system, are transformed into frequency region using the Fourier discrete transformation:

$$\dot{c}_{(r)}\left(n\right) \;=\; \frac{1}{\mathrm{N}}\sum_{k=0}^{\mathrm{N}-1} s_{(r)}\left(k\right)\cdot w\left(k\right)\cdot \exp\left(-j2\pi\frac{nk}{\mathrm{N}}\right) \qquad (1)$$

where $w(k)$ are the coefficients of the weight function used for decrease in leakage of spectrum components in to adjacent frequencies. It should be noted that usage of weight functions with low level of lateral lobes associated with significant impairment of frequency resolution, thus, upon calculation of spectrum samples Eq. (1) it would be useful to decimate spectrum samples, or provide fragmented accumulation of samples (*Tokarev, 1995*).

Finally, the phase spectra of different data sets have random phase deviations, which are not informative in CEME searching. Hence, it is recommended to use periodograms as primary data of detection algorithm of informative CEME components

$$X_{(r)}(n) = \left| \dot{c}_{(r)}(n) \right|. \tag{2}$$

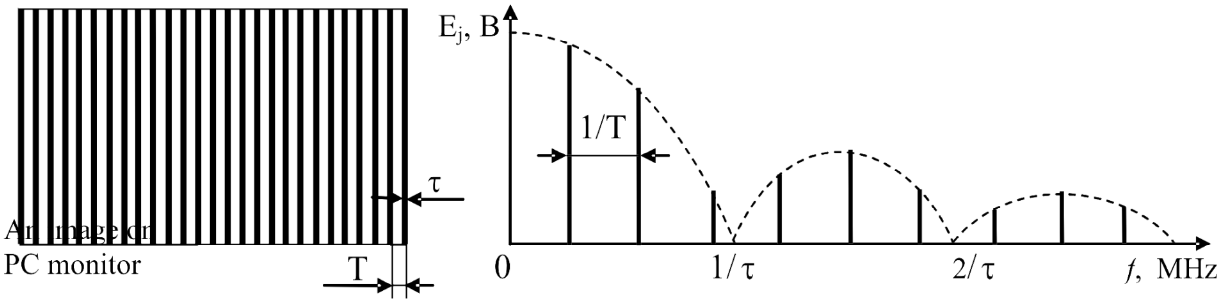


Fig. 1. Schematic view of image and spectrum of data signal intest mode.

2.2. Probability properties of periodogram samples

Searching for informative CEME components is usually performed in wide frequency band of hundreds of megahertz, where the source signal $s_{(r)}(k)$ is a sum of wide band normal noise with huge combination of narrow band signals. In similar cases real and imaginary parts of complex samples(1) are weakly correlated between themselves normal random values, thus, the samples of periodogram (2) should obey generalized Rayleigh distribution:

$$W_{(r)}(x\,;n) = \frac{x}{\sigma_x^2}\exp\left[-\frac{1}{2\sigma_x^2}\left(x^2+\alpha_n^2\right)\right]I_0\left(\frac{\alpha_n x}{\sigma_x^2}\right), \quad x \geq 0, \tag{3}$$

where α_n is the amplitude of signal component at the frequency of the n-th sample, $I_0(.)$ is the Bessel function of imaginary argument of the first kind and zero order, and the parameter σ_x is defined as follows:

$$\sigma_x = \frac{\sigma_n}{\sqrt{N}} \tag{4}$$

where α_n is the effective value of influencing noise.

In addition, the following circumstances should be taken into account :

1. Tested for CEME computer hardware is tested in assembled condition. In particular, upon analysis of monitor the operation of motherboard, processor, PC power unitis in progress. As a consequence, electromagnetic field near CHW is generated by wide combination of signals of complex structure.

   Since the compromising emanations have moderate intensity, the receiving antenna of radio monitoring system should be located upon their search as close as possible to tested equipment, thus providing “successful” receiving of all spectral components of all CHW units (components).

2. Anechoic facilities could be rather rarely applied for investigation into compromising emanations. Upon operation out side anechoic chamber (“normal” conditions) sufficiently rich own spectrum of tested equipment is supplemented by numerous emanations of “external” radio environment.

3. Maximum achievable frequency resolution is limited by technical performances of equipment and equals usually to hundreds of hertz and even to several hundreds of kilohertz per sample.

4. The samples of periodogram (2) of low value, as a rule, slightly influence on the results of analysis of information security with regard to leakage via CEME channel, since (most probable) they correspond to the frequencies where only noise or low intensive compromising emanations are active.

5. Using of generalized Rayleigh distribution in theoretical considerations leads, on the one hand, to rather cumber some calculations (due to the Bessel function), and on the other hand only approximately corresponds to actual situation, since at moderate spectral resolution not one but many "signal" spectrum components fall into frequency interval corresponding to separate sample of periodogram (2).

   Taking into account that

   - at significant amplitude of signal component α_n the generalized Rayleigh distribution is successfully approximated by Gaussian curve;
   - mutual action of closely located narrow band components "normalizes" the behavior of samples of periodogram(2);
   - significant error of the Gaussian approximation of samples at the frequencies where signal components are absent and only noise is active does not result in rough errors in solution of the main problem of information security;

it is possible to conclude that in order to describe properties of the *n*-th sample of periodogram (2) it is allowable and reasonable to apply normal distribution:

$$\mathrm{W}_{(r)}\,(x\,;n) \;\approx\; \frac{1}{\sqrt{2\pi}\cdot\sigma_n}\exp\left[-\frac{1}{2\sigma_n^2}\cdot\left(x-a_n\right)^2\right] \tag{5}$$

where α_n is the parameter characterizing intensity of signal components at the frequency of the *n*-th sample, $\sigma_n$is the value determining the intensity of noise component for the same sample.

Validity of such approximation is definitely confirmed by experimental study of actual observed emanation spectra.

2.3. Combined detection and testing of informativity of CEME components

Detection of all informative CEME, acting in certain frequency range, is based on the use of online programmable toggling of operation mode of tested CHW unit. Let us assume that due to alternative toggling of operation mode of tested unit R_y periodograms are accumulated, corresponding to active (test) mode, and R_z periodograms corresponding to passive mode. Since the test mode provides concentrations of CEME signals in narrow spectral bands, and the samples of periodograms are weekly correlated by frequency, then in order to detect informative CEME components it is allowed to analyze spectral samples independently on each other.

On the basis of values for the *n*-th sample, obtained for test operation mode of considered equipment, we form the vector $\vec{y} = \{y_{(1)}(n), y_{(2)}(n)...y_{(R_y)}(n)\}$; and we combine similar values, obtained in passive operation mode of considered equipment, into the vector $\vec{z} = \{z_{(1)}(n), z_{(2)}(n)...z_{(R_z)}(n)\}$. If at the frequency of the *n*-th sample there is no informative CEME component (hypothesis H_0), then the samples of the vectors $\vec{y}$ and $\vec{z}$ should obey one and the same distribution (5) with the parameters a_{n0} and σ_{n0}. If the hypothesis H_1 about informativity of CEME component at the frequency of the *n*-th sample is valid, then the parameters a_{ny}, $\sigma_{n1}$of $\vec{y}$ vector distribution and the parameters a_{nz}, σ_{n1} of $\vec{z}$ vector distribution will differ from each other. Hence, the likelihood functions of the obtained data are as follows:

$$\mathrm{L}_0(\vec{y},\vec{z}) \;=\; \frac{1}{\left(\sqrt{2\pi}\cdot\sigma_{n0}\right)^{\mathrm{R}_y+\mathrm{R}_z}}\cdot\exp\left[-\frac{1}{2\sigma_{n0}^2}\cdot\left(\sum_{r=1}^{\mathrm{R}_y}\left(y_{(r)}(n)-a_{n0}\right)^2+\sum_{r=1}^{\mathrm{R}_z}\left(z_{(r)}(n)-a_{n0}\right)^2\right)\right] \tag{6}$$

$$\mathrm{L}_1(\vec{y},\vec{z}) \;=\; \frac{1}{\left(\sqrt{2\pi}\cdot\sigma_{n1}\right)^{R_y+R_z}}\cdot\exp\left[-\frac{1}{2\sigma_{n1}^2}\cdot\left(\sum_{r=1}^{R_y}\left(y_{(r)}(n)-a_{ny}\right)^2+\sum_{r=1}^{R_z}\left(z_{(r)}(n)-a_{nz}\right)^2\right)\right] \tag{7}$$

Maximum likelihood estimations of the parameters a_n and σ_n can be written as follows:

$$a_{n0}^{*} = \frac{1}{\mathrm{R}_y + \mathrm{R}_z} \cdot \left(\sum_{r=1}^{\mathrm{R}_y} y_{(r)}(n) + \sum_{r=1}^{\mathrm{R}_z} z_{(r)}(n) \right) \tag{8}$$

$$\left(\sigma_{n0}^{*}\right)^2 = \frac{1}{\mathrm{R}_y + \mathrm{R}_z} \cdot \left(\sum_{r=1}^{\mathrm{R}_y} \left(y_{(r)}(n) - a_{n0}^{*} \right)^2 + \sum_{r=1}^{\mathrm{R}_z} \left(z_{(r)}(n) - a_{n0}^{*} \right)^2 \right) \tag{9}$$

$$a_{ny}^{*} = \frac{1}{\mathrm{R}_y} \cdot \sum_{r=1}^{\mathrm{R}_y} y_{(r)}(n) \tag{10}$$

$$a_{nz}^{*} = \frac{1}{\mathrm{R}_z} \cdot \sum_{r=1}^{\mathrm{R}_z} z_{(r)}(n) \tag{11}$$

$$\left(\sigma_{n1}^{*}\right)^2 = \frac{1}{\mathrm{R}_y + \mathrm{R}_z} \cdot \left(\sum_{r=1}^{\mathrm{R}_y} \left(y_{(r)}(n) - a_{ny}^{*} \right)^2 + \sum_{r=1}^{\mathrm{R}_z} \left(z_{(r)}(n) - a_{nz}^{*} \right)^2 \right) \tag{12}$$

Substituting the set of unknown parameters a_n and σ_n, in Eqs. (6) and (7) by their maximum likelihood estimations the likelihood ratio of hypotheses H_1 and H_0 can be presented as follows:

$$l(\vec{x},\vec{y}) = \frac{\mathrm{L}_1(\vec{x},\vec{y})}{\mathrm{L}_0(\vec{x},\vec{y})} = \left(\frac{\sigma_{n0}^{*}}{\sigma_{n1}^{*}} \right)^{\mathrm{R}_y + \mathrm{R}_z} \tag{13}$$

Therefore, optimum in terms of maximum likelihood algorithm of solution about component informativity at the frequency of the *n*-th sample of the observed periodograms assumes comparison statistic (13) with the decision threshold. In addition, the exponent in Eq. (13) is a constant in dependent on the results of measurements and the likelihood ratio is a monotonous function of the expression $\left(\sigma_{n0}^{*}/\sigma_{n1}^{*}\right)^2$.

3. RESULTS AND DISCUSSION

3.1. Resultant algorithm of validation of informativity of individual spectral components

After simple transformations the algorithm of combined detection and testing of informativity of CEME components can be written as follows:

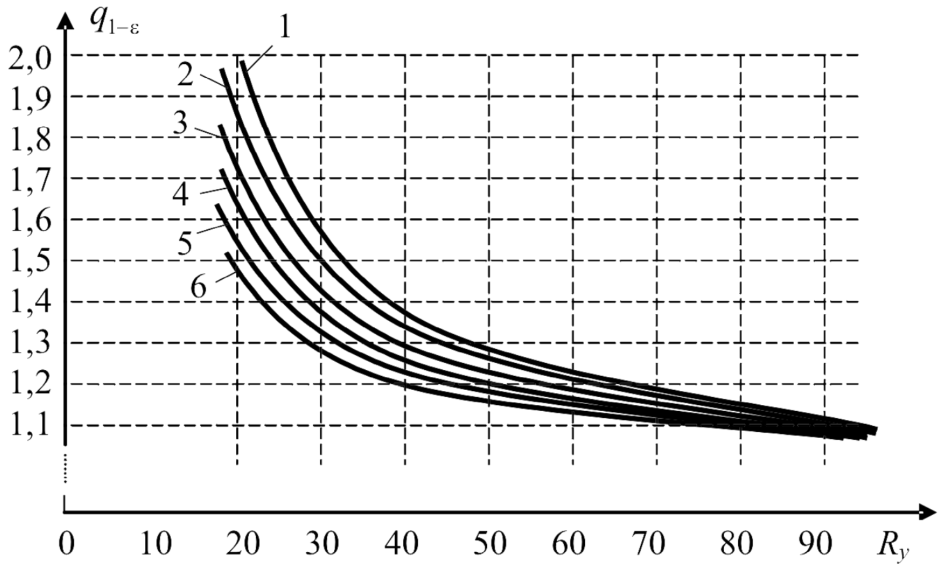
$$\mathrm{Q}_{yz}(n) = \frac{\sum_{r=1}^{\mathrm{R}_y} y_r^2(n) + \sum_{r=1}^{\mathrm{R}_z} z_r^2(n) - \frac{1}{\mathrm{R}_y + \mathrm{R}_z} \cdot \left(\sum_{r=1}^{\mathrm{R}_y} y_r(n) + \sum_{r=1}^{\mathrm{R}_z} z_r(n) \right)^2}{\left(\sum_{r=1}^{\mathrm{R}_y} y_r^2(n) - \frac{1}{R_y} \left(\sum_{r=1}^{\mathrm{R}_y} y_r(n) \right)^2 \right) + \left(\sum_{r=1}^{\mathrm{R}_z} z_r^2(n) - \frac{1}{\mathrm{R}_z} \left(\sum_{r=1}^{\mathrm{R}_z} z_r(n) \right)^2 \right)} \begin{array}{c} \mathrm{H}_1 \\ > \\ < \\ \mathrm{H}_0 \end{array} \mathit{Thresh}, \tag{14}$$

where *Thresh* is the selected decision threshold.

Contrary to the a forementioned typical procedure, which assumes searching for all CEME components and subsequent consecutive testing of all detected components for informativity by means of individual narrow band processing, the algorithm (14) without any additional testing detects only informative CEME components, automatically ignoring other non-informative components. This is a significant advantage in searching speed of informative CEME in comparison with typical procedure.

3.2. Selection of detection threshold of informative CEME

Probability properties of statistics $\mathrm{Q}_{yz}(n)$ for the case of absence of informative CEME components are illustrated in Fig. 2.



$1 - \varepsilon = 5{\cdot}10^{-7}$; $2 - \varepsilon = 10^{-6}$; $3 - \varepsilon = 5{\cdot}10^{-6}$; $4 - \varepsilon = 10^{-5}$; $5 - \varepsilon = 5{\cdot}10^{-5}$; $6 - \varepsilon = 10^{-4}$

Fig. 2. Quantiles $q_{1-\varepsilon}$ of distribution statistics $Q_{yz}(n)$ for non-informative CEME components as a function of number of periodograms $R_y = R_z = R$.

The quantiles for actual values of ε illustrated in Fig. 2 correspond to the probability of false alarm, obtained at individual testing of single sample of spectrum with the number *n*. Upon processing of wide frequency range, containing many thousands of samples, probability of false detection of informative CEME components will be drastically higher. In particular, this means that the higher is the frequency resolution of radio monitoring equipment, the higher is the number of spectral samples representing the radio environment in the considered frequency range and, hence, the higher is the threshold *Tresh* required for maintaining of integral probability of false detection of informative CEME components. Taking into consideration that at $N_{all} >> 1$ and $\varepsilon \approx 0$ the expression $(1-\varepsilon)^{N_{all}} \approx 1 - N_{all} \cdot \varepsilon$ is valid, we conclude that in order to provide integral probability of false alarm P_{fa} the allowed probability of threshold exceeding by singe non-informative statistics $Q_{yz}(n)$ should equal to:

$$\varepsilon \le P_{fa}/N_{all}\,, \tag{15}$$

where N_{all} is the total number of tested spectral samples in overall tested frequency range.

Let us account additionally that single cases of false detection of informativeCEME componentsin the course of specialized study are not so hazardous, as a rule, they slightly increase the time of data acquisition about intensity distribution of informative CEME in frequency range. Taking this into account, in the case of application of relatively inexpensive systems of radio monitoring, manufactured earlier than 2010 (*Radio Monitoring*, 2009), it was decided to apply the following empirical equation for threshold selection:

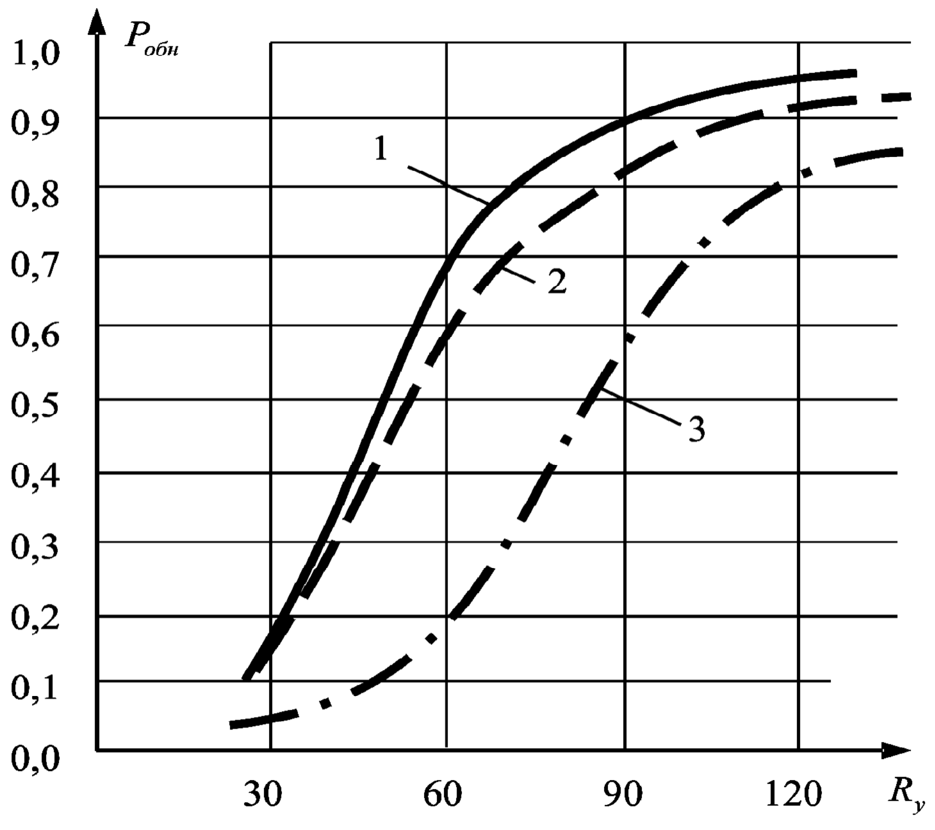
$$\text{Thresh} = K_1 + \frac{K_2}{R - K_3} \tag{16}$$

where the values of coefficients $K_1 \ldots K_3$ are selected in accordance with the frequency resolution used upon data acquisition. Subsequent results were obtained with the coefficients $K_1 = 1{,}02$; $K_2 = 9$; $K_3 = 6$ for the cases when the interval between spectral samples was 3.125 kHz and at the coefficients $K_1 = 1{,}02$; $K_2 = 13$; $K_3 = 3$ as applied to increased by eight times spectral resolution which provides decrease in the frequency interval between spectral samples to 390 Hz. As follows from the comparison of thresholds *Thresh* with probabilities in Fig. 2, for similar threshold the probability of occurrence of single false detected informative CEME for the frequency ranges of 100 MHz is 25% (or less), which does not create problems in the course of specialized study but facilitates detection of informative CEME components of low intensity.

3.3. Operation quality of algorithm of combined detection and testing of informativity of CEME components

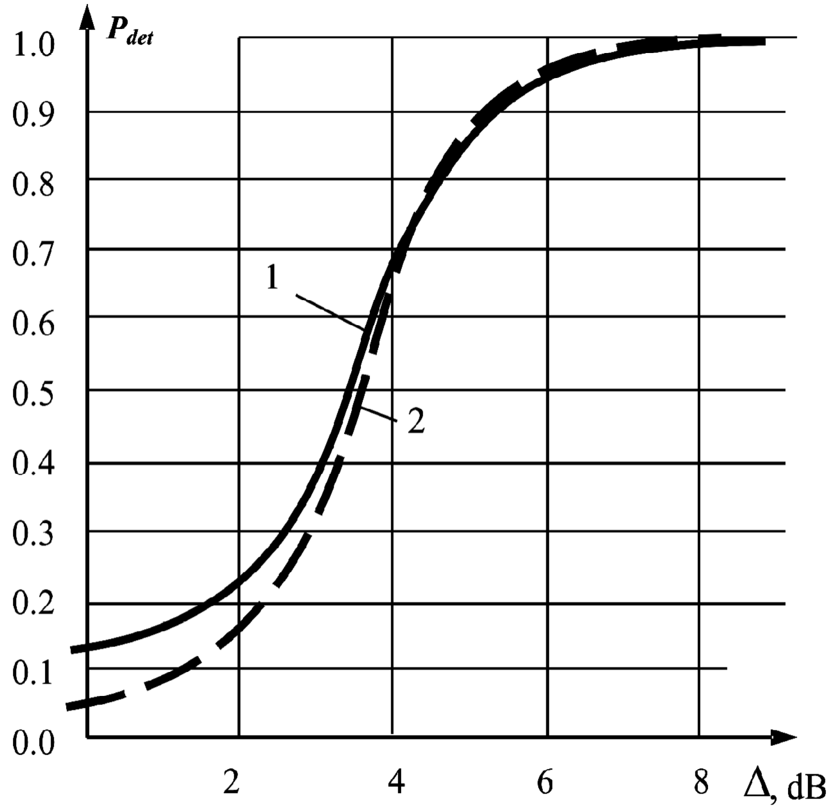
Physical simulation of the new algorithm (14) demonstrated that reliability of detection of informative components depends on the number of processed periodograms, their frequency resolution and intensity of detected CEME components. In the below diagrams the parameter Δ characterizes the intensity of detected CEME components. It is determined numerically by the difference in decibels between spectral samples corresponding to background noise and CEME component to be detected. Figure 3, as applied to two tested values of frequency resolution Δ*f* of radio monitoring equipment, illustrates probability of detection of informative CEME components as a function of number of accumulated and processed periodograms. Figure 4 approximately compares the detection quality of informative CEME components upon application of algorithm (14) and two-stage procedure described in Introduction.

In accordance with Fig. 4 at high amount of accumulated periodograms the recommended above thresholds provide the detection probability of informative CEME components more than 95% for the components with excess over panorama Δ equal or higher than 6 decibels. Weaker CEME components are also detected, but, of course, with lower probability. Due to accumulation and use of additional periodograms this probability can be improved, however, it would be more efficient to apply spectra with higher frequency resolution. When high resolution is applied, significantly lower noise power faction fall with in each sample of amplitude spectrum, which enables detection of significantly weaker components. The cost of the mentioned improvement is increase in time and hardware expenditures required for data processing.



1 – Δ = 0 dB, Δ*f* = 390 Hz; 2 – Δ = 4 *d*B, Δ*f* = 3125 Hz; 3 – Δ = 3 dB, Δ*f* = 3125 Hz

Fig. 3. Probability of detection of informative CEME components for the developed algorithm.



1 – developed algorithm ($R_y = R_z = 30$, $\Delta f = 390$ Hz); 2– typical two-stage procedure

Fig. 4. Comparison of detection probabilities of informative CEME components for new algorithm and for typical procedure.

4. CONCLUSIONS

The proposed algorithm of combined detection and testing of informativity of CEME components is oriented at the use of radio monitoring equipment providing spectral analysis of environment with high frequency resolution (preferably, several hundreds of Hertz or less) and software enabling automatic toggling of tested CHW units from passive state to active and vice versa. With the aim of reliable detection of informative CEME components for each tested unit the number of periodograms accumulated upon cyclic variation of current operation mode of tested unit should equal to several tens (at least 30) both for active and inactive operation mode of a unit. Though, the use of comparatively low number of spectra with high frequency resolution can provide better results than accumulation of many data sets with low spectral resolution.

The analyzed algorithm is one-stage and detects informative CEME componentsin all frequency band of spectral analysis without usage of narrow band processing of individual CEME components. Qualitative properties of the new algorithm are comparable with the results of conventional two-stage procedure of detection of CEME components, and the obtained search rate is significantly higher.

In the case of the applied threshold the algorithm sensitivity is some what excessive. At high number of accumulated periodograms ($R \geq 90$) and high frequency resolution this algorithm reliably detects CEME components, which in active (test) mode in direct proximity to CHW have intensity coinciding with background noise, that is, signal–noise ratio for them is 0 dB. Under ambient conditions and with accounting for attenuation of electromagnetic field upon moving of observation point from tested CHW such CEME components can not be dangerous from the point of view of information leakage.Thus, in subsequent studies, it would be reasonable to optimize the procedure of threshold selection aiming at detection of only hazardous CEME components from the point of view of information leakage.

5. REFERENCES

1. Ahsan, A., Islam R. & Islam, A. (2014) A Countermeasure for Compromising Electromagnetic Emanations of Wired Keyboards. In*17th Int’l Conf. on Computer and Information Technology, 22-23 December 2014*, Dhaka, Bangladesh: Daffodil International University.
2. Anishchenko, A.N., Lyashenko, A.V., Solopov, P.A.,&Sotov, L.S. (2014) Risk Reducing of Information Leakage Due to Compromising Emanation.Geteromagn. Elektron.. – 2014 – #17 – pp. 66-77.Retrieved from http://hmm.sgu.ru/sites/default/files/minimizaciya_riskov_utechki_informacii_iz-za_pobochnyh_ elektromagnitnyh_ izlucheniy_ personalnogo_komyutera.pdf
3. Asotov D.V., Matveev B.V., Chernoyarov O.V., Lysina E.A. Radio Waves Attenuation Model for a Ray Approximation // 2015 International Siberian Conference on Control and Communications (SIBCON). Proceedings. – Omsk: Omsk State Technical University. Russia, Omsk, May 21"23, 2015. – 5 p.
4. Asotov D.V., Matveev B.V., Faulgaber A.N., Salnikova A.V. The Exact and Approximate Task Solution of a Ray Tracing at Their Transition in a Medium With Finite Conductivity // 25th International Crimean Conference Microwave and Telecommunication Technology (CriMiCo-2015), Conference Proceedings, 2015, vol. 2, pp. 1200-1201.
5. Bekhtin, M.A. (2009) System of Detection of Adverse Electromagnetic Emanation. Candidate Thesis, Specialty: 05.12.04 Radiotechnics, including TV systems and devices, Moscow, 2009
6. Buzov, G. A., Kalinin S.V., and Kondrat‘ev, A.V. (2005) Protection against Information Leakage via Engineering Channels. Guidebook. (GoryachayaLiniyaTelekom, Moscow, 2005. ISBN 5-93517-204-6).
7. Cazanaru, D., Cosereanu, L., &Szilagry A. (2011) Evaluation of the compromising radiation by electromagnetic compatibility tests *U.P.B. Sci. Bull., Series A, Vol. 73, Iss. 2, 2011* ISSN 1223-7027 Retrieved from http://www.scientificbulletin.upb.ro/rev_docs_arhiva/full10813.pdf
8. Dmitryiev, U.A.,Stepanyan, A.B., & FisenkoU.K. (2013) Control of Protection of Confidential Information for Input from the PC Keyboard.// Iskusstv. Intellekt, – 2013 – # 3 – pp. 549-553. Retrieved from http://dspace.nbuv.gov.ua/bitstream/handle/123456789/85079/62-Dzmitryiev.pdf
9. Ermakova, I.M., & Shlegel.O.A. (2008) The characteristic of technical channels of outflow and not authorized access to the information. Retrieved from tolgas.ru/site/upload/file/kaf_se/n02/08.doc
10. Filin, N.A., Minin, I.V.,&Minin, O.V. (2013) Guidelines for software development and document systems for measuring spurious electromagnetic radiation terms of guidance documents to protect information, metrology and gostInterexpo Geo-Sibir’. – 2013 – Volume 5 – #2 – pp. 19-25. Retrieved from http://cyberleninka.ru/article/n/rekomendatsii-po-razrabotke-programmnogo-obespecheniya-i-tehnicheskoy-dokumentatsii-sistem-izmereniya-pobochnogo-elektromagnitnogo
11. Frankland R. (2011) Side Channels, Compromising Emanations and Surveillance.*Current and future technologies Technical Report RHUL–MA–2011–07 8th March 2011*.http://www.ma.rhul.ac.uk/static/techrep/2011/RHUL-MA-2011-07.pdf
12. Gorobets, N.N.,&Trivaylo, A.V. (2009) Compromising emanations: Overview and system analysis // Vestn. Kharkov National University. Series: RadiophysicsandElectronics. No. 883, Issue15, 2009.PP. 83-88
13. Horev, A.A. (2007)EstimationofProtectionEfficiencyofAuxiliaryTechnicalAids// Spec. Technique. – 2007 – #2. Retrieved fromwww.ess.ru/sites/default/files/files/articles/2007/02/2007_02_08.pdf
14. Horev, A.A. (2014) Evaluation of the possibility of detection side compromising electromagnetic emanations video PC // Reports of Timsk State University of Control Systems and Radioelectronics. – 2014. – #2 – pp. 207-213.Retrieved from http://cyberleninka.ru/article/n/otsenka-vozmozhnosti-obnaruzheniya-pobochnyh-elektromagnitnyh-izlucheniy-videosistemy-kompyuter
15. IvanovV.P. (2007)DevicesofTEMPEST RadioDeceptionon the Basis of Ultra-Wideband Noise Generator // Izv. South Federal University. technical Science. Complex protection of software applications, pp. 47-54. Retrieved from http://cyberleninka.ru/article/n/ustroystva-radiomaskirovki-pemin-na-osnove-sverhshirokopolosnyh-generatorov-shuma
16. Korolev, M.V. (2013) Method of Calculation of the Zone Boundary protection of Information in the Far Field Radiation Source//SecurityofDataTechnologies (Publishing House: Tsentrekspertizy, Moscow ISSN: 2074-7128. – 2013). – #1. – pp. 58-62. Retrieved from pvti.ru/data/file/bit/2013/2013_1/part_17.pdf
17. Kuhn, M.G. (2003) Compromising emanations: eavesdropping risks of computer displays. Retrieved from http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf
18. Kuhn, M.G., &Anderson, R.J. (1998) Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations In*Information hiding* (pp 124-142) Second International Workshop, IH’98, Portland, Oregon, USA. http://dx.doi.org/10.1007/3-540-49380-8. Retrieved from http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf

19. Lykov, Yu. V. andSyagaeva, O, O, (2012) Analysis of TEMPEST Sources in Modern PC// Radiotekhn.- 2012. - Issue. 169. - Ñ. 196-207. - http://nbuv.gov.ua/UJRN/rvmnts_2012_169_30.

20. Meynard, O., Guilley, S., Danger, J.-L.,Hayashi Yu-I.&Homma, N. (2012) Characterization of the Information Leakage of Cryptographic Devices by Using EM Analysis.In Bashir S.O. *Electromagnetic Radiation* (pp. 225-248), ISBN 978-953-51-0639-5, http://dx.doi.org/10.5772/38309.

21. Nowosielski, L., &Wnuk, M.(2014) Compromising Emanations from USB 2 Interface // PIERS Proceedings, Guangzhou, China, August 25–28, 2014

22. Filippovich A.G. (2014) Analysis of Adverse Radio Emanations of Processing Aids in Near, Intermediate and Far Region for Data Protection / Cand.thesis, Specialty 05.13.19 and 05.12.07 / Minsk 2014

23. Poyarkov, L. A., Babkin A. N., Ivanov S.M.(2012) A comparative analysis of different indicators for the evaluation of the security of the information from leaking through stray electromagnetic radiation from a single-digit and multiple bit digital signals //Vestn. Voronezh Insititute of Ministry of Internal Affairs of Russia . – 2012. – #4.Retrieved fromhttp://cyberleninka.ru/article/n/sravnitelnyy-analiz-razlichnyh-pokazateley-otsenki-zaschischennosti-informatsii-ot-utechki-za-schet-pobochnyh-elektromagnitnyh

24. Przesmycki, R.(2014) Measurement and Analysis of Compromising Emanation for Laser Printer // Progress In Electromagnetics Research Symposium Proceedings, Guangzhou, China, Aug. 25–28, 2014.

25. Soft- and hardware complex for searching of adverse electromagnetic emanations: “Navigator”, Description of application. Retrieved from http://www.nelk.ru/files/Opisaniie_primienieniia.pdf

26. Radio Monitoring. Problems, Methods, and Equipment(2009) A volume 43 in the nanostructure Science and Technology series. ISBN 978-0-387-98099-7, Springer Dordrecht Heidelberg London New York, 2009.

27. Rohatgi, P. (2009) Electromagnetic Attacks and Countermeasures. In Cryptographic Engineering, pp. 407-430.http://dx.doi.org/10.1007/978-0-387-71817-0 15

28. Comparative analysis of methods and tools of measurement automation upon specialized studies of computer aids on the basis of TEMPEST. Retrieved from http://www.bnti.ru/showart. asp? aid = 540& lvl = 04.02.01.

29. Sudarikov, A.V., Romashchenko M.A. (2011) The review of technical devices for measurement of characteristics of electromagnetic fields. In *Proceedings of International Symposium”Reliability and Quality”*. Publishing House of Penza Srare University, Penza, 2011.-Vol.2.-PP.213-215 Retrieved from http://cyber leninka.ru/article/n/obzor-tehnicheskih-ustroystv-dlya-izmereniya-harakteristik-elektromagnitnyh-poley

30. Sokolov, R.I., Astretsov, D.V., Kobyakov, V.U. Potential detection special component of compromising emanations signal USB keyboard interface // 2nd International conference of students, post graduates and young researchers” Information technologies, telecommunications and control systems” : Proceedings. — Ekaterinburg: [UrFU], 2016. — PP. 152-160. Retrievedfromhttp://elar.urfu.ru/bitstream/10995/36241/1/ittsm-2016-20.pdf

31. Tokarev, A.B. (1995) Development of digital algorithms of wide band radio motoring for data transfer systems/ Cand. Thesis, Specialty 05.12.04 “Radiotekhnika». Voronezh, 1995

32. Tupota, V.I., KozminV.A., &Tokarev, A.B. (2006) Application of ARK-D1TI multifunctional complex for estimation of data protection against leakage via TEMPEST channel // Spec. Tekhn. – 2006. – # 1. – PP. 38-46.

33. Ulas C., Sahin, S., Memisoglu, E., Asýk, U.,Karadeniz, C.,Kýlýc, B.,&Sarac. U.(2014) Automatic TEMPEST test and analysis system design. *International Journal on Cryptography and Information Security* (IJCIS), Vol. 4, No. 3, September 2014.http://dx.doi.org/10.5121/ijcis.2014.4301.

34. Van Eck, Wim (1985). ”Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk ?” *Computers & Security 4 (4)*: pp. 269–286. http://dx.doi.org/10.1016/0167-4048(85)90046-X.

35. Vuagnoux, M., &Pasini, S. (2009) Compromising Electromagnetic Emanations of Wired and Wireless Keyboards. In*18th USENIX Security Symposium. Montreal, Canada, August 10-14, 2009.* Retrieved from https://www.usenix.org/legacy/event/sec09/tech/full_papers/vuagnoux.pdf

36. Vuagnoux, M., & and Pasini, S. (2010) An improved technique to discover compromising electromagnetic emanations. In: Electromagnetic Compatibility Symposium (Emc 2010), Fort Lauderdale, USA, p. 121-126. (ISBN: 978-1-4244-6307-7). Retrieved from https://infoscience.epfl.ch/record/171931.

37. Zidong,Zh.,Yuanhui, Yu.Quality Evaluation Model of Information Reconstruction via Electromagnetic Emanation.*TELKOMNIKA Indonesian Journal of Electrical Engineering Vol.12, No.3, March 2014*. (pp. 1960-1964) http://dx.doi.org/10.11591/telkomnika.v12i3.4467.