УДК 538.3+537.86

COMPROMISING EMANATIONS: OVERVIEW AND SYSTEM ANALYSIS

N.N. Gorobets, A.V. Trivaylo

V. Karazin National University of Kharkov, 4, Svoboda sq., Kharkov, 61077, Ukraine
e-mail: Nikolay.N.Gorobets@univer.kharkov.ua

Received 4 Sseptember.2009

The problem of compromising radiation of spurious signals in the near, intermediate and far zones of observation in time domain are considered. The Compromising emanation system analysis for finding spurious radiation is proposed. The goal of the given approach is to speed the development of technical protection of information. In approximation of the given current distribution it has been suggested a solution considering the influence of the near-field effects upon directional characteristics of spurious signals radiation. The application of the new method allows us to investigate compromising of technical means in time and frequency domain.

KEYWORDS: compromising emanations, near-field-zone, electromagnetic, radiation, time domain

Рассмотрена задача побочных электромагнитных излучений опасных сигналов в ближней, промежуточной и дальней зонах. Проанализированы экспериментальные данные побочных электромагнитных излучений различных технических средств. Предложен системный анализ для нахождения и изучения побочных электромагнитных излучений. Целью данного подхода является создание корректной теоретической базы в области технической защиты информации. Рассмотрен метод векторных нестационарных потенциалов для нахождения компонент электромагнитного поля опасных сигналов в ближней, промежуточной и дальней зонах излучения. Применение нового метода позволяет исследовать побочные электромагнитные излучения технических средств во временной и в частотной области.

КЛЮЧЕВЫЕ СЛОВА: побочные электромагнитные излучения, ближняя зона, электродинамика, излучение, временная область

Розглянуто задачу побічних електромагнітних випромінювань небезпечних сигналів у ближній, проміжній та дальній зонах. Проаналізовано експериментальні дані побічних електромагнітних випромінювань різних технічних засобів. Запропонований системний аналіз для знаходження та вивчення побічних електромагнітних випромінювань. Метою даного підходу є створення коректної теоретичної бази в галузі технічного захисту інформації. Розглянуто метод векторних нестаціонарних потенціалів для знаходження компонент електромагнітного поля небезпечних сигналів у ближній, проміжній та дальній зонах випромінювання. Застосування нового методу дозволяє досліджувати побічні електромагнітні випромінювання технічних засобів у часовій і в частотній області.

КЛЮЧОВІ СЛОВА побічні електромагнітні випромінювання, ближня зона, електродинаміка, випромінювання, часова область

INTRODUCTION

Electronic equipment can emit unintentional radio signals from which eavesdroppers may reconstruct processed data at some distance. Electromagnetic radiation as a computer security risk was mentioned in the open literature as early as 1966 [1], but without technical details on specific risks and eavesdropping techniques. Probably the first more detailed public description of compromising emanation risks appeared in Sweden around 1982 and in 1984 a Swedish government committee issued an 18-page booklet in Swedish that informed the wider business community about the threats of acoustic, radiated, conducted and, in particular, video emissions [2].

The concept was brought to the attention of the broader public by a 1985 paper [3], in which van Eck demonstrated that the screen content of a video display unit could be reconstructed at distance using low-cost home built equipment, namely a TV set whose sync-pulse generators were replaced by manually controlled oscillators.

Smulders showed that shielded RS-232 cables can be eavesdropped at a distance [4]. Connection cables form resonant circuits consisting of the induction of the cable and the capacitance between the device and ground; these are excited by the high-frequency components in the edges of the data signal, and the resulting short HF oscillations emit electromagnetic waves.

Nearly half a century ago, military organizations introduced “Tempest” emission-security test standards to control information leakage from unintentional electromagnetic emanations of digital electronics. The nature of these emissions has changed with evolving technology; electromechanic devices have vanished and signal frequencies increased several orders of magnitude. Interest in compromising emanations and other aspects of hardware security surfaced again in the 1990s with the mass-market introduction of tamper-resistant cryptographic modules.

The purpose of this paper – is to give the experimental data review and to develop physico-mathematical model of spurious signals radiation based on correct theoretical methods.

COMPROMISING EMANATIONS OF COMPUTER DISPLAYS

It is shown [5] that the information displayed on a modern cathode-ray tube computer monitor can be reconstructed by an eavesdropper from its distorted or even diffusely reflected light using easily available components such as a photomultiplier tube and a computer with suitably fast analog-to-digital converter.

The intensity of the light emitted by a raster-scan screen as a function of time corresponds to the video signal convolved with the impulse response of the phosphors. Experiments with a typical personal computer color monitor showed that enough high-frequency content remains in the emitted light to permit the reconstruction of readable text by deconvolving the signal received with a fast photosensor. These optical compromising emanations can be received even after diffuse reflection from a wall. Due to shot-noise limits, the eavesdropping from diffuse reflections of display light seems only applicable in relatively dark environments and is even then limited to less than a few tens or hundreds of meters distance, but that alone might already be of practical concern in some situations. Better eavesdropping distances even under office-light conditions become possible with a direct line of sight, which might include minor distortions such as frosted glass that would otherwise be deemed sufficient to frustrate projective observation.

Electromagnetic eavesdropping of computer displays - is not restricted to cathode-ray tubes. Modern flat-panel displays can be at least as vulnerable. They are equally driven by repetitive video signals in frequency ranges where even shielded cables leak detectable radio waves into the environment. Nearby eavesdroppers can pick up such compromising emanations with directional antennas and wideband receivers. Periodic averaging can lift a clearly readable image out of the background noise. The serial Gbit/s transmission formats used by modern digital video interfaces in effect modulate the signal, thereby making it even better suited for remote reception than emanations from analog systems.

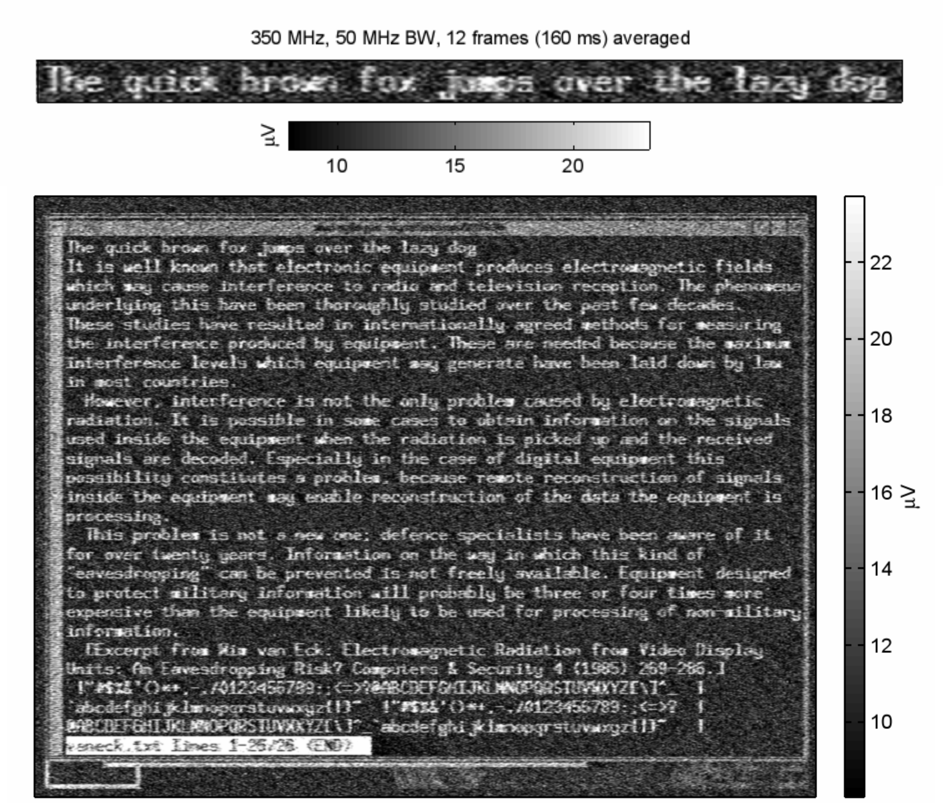
A new form of compromising emanations from video displays was discovered more recently. The high-frequency variations of light emitted by a CRT can carry enough information about the video signal to permit the reconstruction of readable text. Under low background illumination, this is practical even after diffuse reflection from nearby surfaces. LCDs are not vulnerable to this particular risk, not only because their pixels react much slower than CRT phosphors, but also because these technologies update all pixels in a row simultaneously. This makes it impractical to separate the contribution of individual pixels in a row to the overall light emitted.

Flat-panel displays are widely believed to pose no electromagnetic eavesdropping risk either. Two facts may contribute to such an assumption. Firstly, FPDs lack deflection coils, which makes them - compared to CRTs - "low radiation" devices in the frequencies below 400 kHz, where field strengths are limited by a Swedish ergonomic standard. Secondly, LCDs operate with low voltages and - unlike CRTs -do not amplify the video signal by a factor of about 100 to drive a control grid that modulates an electron beam.

The experiments reported in [6] demonstrate that some types of flat-panel display do pose a realistic eavesdropping risk. In particular, with some modern video interfaces, it is quite easy to configure the display of text in a way that maximizes the leaking signal strength. This makes emanations from these displays even easier to receive than those of modern CRTs. In the experiments [6] compromising radio emanations from a laptop LCD and from a desktop LCD that is connected to its PC graphics card with a Digital Visual Interface (DVI) cable were analyzed. For example, Figure 1 shows the result, an easily readable view of an extern window that shows some test text. The received signal amplitude of about $12\,\mu V$ corresponds with antenna to field strength of $39 dB\mu V / m$.

The eavesdropping risk of flat-panel displays connected via Gbit/s digital interfaces to their video controller is at least comparable to that of CRTs. Their serial transmission formats effectively modulate the video signal in ways which provide eavesdroppers with even better reception quality.

Also it was concluded [7] that due to the redundancy of a periodic signal and due to the ultra-wideband nature of compromising emanations from digital base-band signals, meaningful emission limits end up near the performance limits of modern spectrum analyzers. If the protection is to be achieved by shielding and attenuation, the permitted signal power must be several million times lower than what civilian radio-interference standards permit.


350 MHz, 50 MHz BW, 12 frames (160 ms) averaged
The quick brown fox jumps over the lazy dog
µV
10
15
20
22
20
18
16
14
12
10
µV

```
The quick brown fox jumps over the lazy dog
It is well known that electronic equipment produces electromagnetic fields
which may cause interference to radio and television reception. The phenomena
underlying this have been thoroughly studied over the past few decades.
These studies have resulted in internationally agreed methods for measuring
the interference produced by equipment. These are needed because the maximum
interference levels which equipment may generate have been laid down by law
in most countries.
  However, interference is not the only problem caused by electromagnetic
radiation. It is possible in some cases to obtain information on the signals
used inside the equipment when the radiation is picked up and the received
signals are decoded. Especially in the case of digital equipment this
possibility constitutes a problem, because remote reconstruction of signals
inside the equipment may enable reconstruction of the data the equipment is
processing.
  This problem is not a new one; defence specialists have been aware of it
for over twenty years. Information on the way in which this kind of
"eavesdropping" can be prevented is not freely available. Equipment designed
to protect military information will probably be three or four times more
expensive than the equipment likely to be used for processing of non-military
information.
  [Excerpt from Wim van Eck: Electromagnetic Radiation from Video Display
Units: An Eavesdropping Risk? Computers & Security 4 (1985) 269-286.]
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_  |
`abcdefghijklmnopqrstuvwxyz{|}~  !"#$%&'()*+,-./0123456789:;<=>?  |
@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~   |
vaneck.txt Lines 1-26/26 (END)
```

Fig. 1. Text signal received from a 440CDX laptop at 10 m distance through two intermediate offices (3 plasterboard walls).

The experiments and analysis of the interception of personal computer's display image using emanation of electromagnetic wave are described in [8]. From the result with using a near magnetic field probe, it was shown that the slight difference in the synchronous frequency of video signal among PCs will become the key which recognizes the target. Based on the results of the experiments on screen interception from electromagnetic emissions presented in the [8], it was concluded that: 1) positions from which electromagnetic waves emanate vary depending on the housing material and shape of the target; 2) differences between CRT and LCD monitors do not affect the difficulty of interception.

COMPROMISING ELECTROMAGNETIC EMANATIONS OF KEYBOARDS

Computer keyboards are often used to transmit confidential data such as passwords. Since they contain electronic components, keyboards eventually emit electromagnetic waves. These emanations could reveal sensitive information such as keystrokes. To determine if wired and wireless keyboards generate compromising emanations the electromagnetic radiations emitted when keys are pressed was measured. The technique generally used to detect compromising emanations is based on a wide-band receiver, tuned on a specific frequency. However, this method may not be optimal since a significant amount of information is lost during the signal acquisition. More correct approach is to acquire the raw signal directly from the antenna and to process the entire captured electromagnetic spectrum. Thanks to this method, it can be detected four different kinds of compromising electromagnetic emanations generated by wired and wireless keyboards. These emissions lead to a full or a partial recovery of the keystrokes. In the paper [9] 12 different keyboard models bought between 2001 and 2008 (PS/2, USB, wireless and laptop) in different setups: a semi-anechoic chamber, a small office, an adjacent office and a flat in a building have been tested. They was all vulnerable to at least one of the four attacks. The best attack successfully recovers 95% of the keystrokes of a PS/2 keyboard at a distance up to 20 meters, even through walls. Most of modern computer keyboards generate compromising emanations (mainly because of the manufacturer cost pressures in the design). Hence, they are not safe to transmit confidential information.

There are 4 different ways (including the Kuhn attack) to fully or partially recover keystrokes from wired keyboards, even through walls. Figure 2 gives the maximum range for the four techniques measured in the office (here FETT – Falling Edge Transition Technique, GTT – Generalized Transition Technique, MT – Modulation Technique, MST – Matrix Scan Technique [9]).

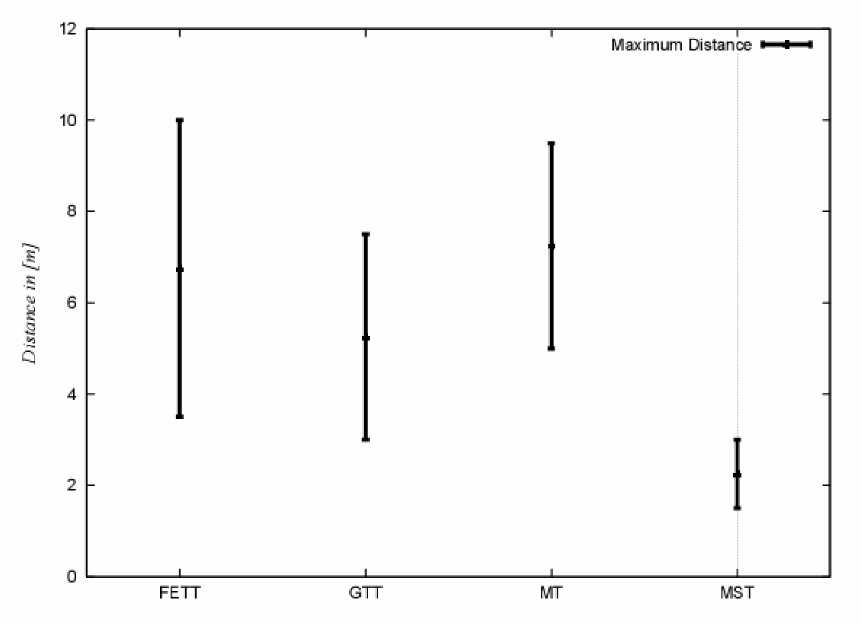


Fig. 2. Maximum distance ranges, from the least vulnerable keyboard to the most vulnerable keyboard, to successfully recover 95% of the keystroke according to the techniques (in the office with the biconical antenna).

Acoustic compromising emanations from keyboards have been studied as well. Asonov and Agrawal [10] discovered that each keystroke produces a unique sound when it is pressed or released and they presented a method to recover typed keystrokes with a microphone. This attack was later improved. Even passive timing analysis may be used to recover keystrokes. A risk of compromising emission from keyboards has been postulated by Kuhn and Anderson [11].

SYSTEM ANALYSIS OF COMPROMISING EMANATIONS

Despite of a lot of experimental data there is no correct mathematical model of compromising emanations both in the near and far-field zones of observations. Currently under the special researches it is necessary to measure level of compromising emanations and calculate special radius R_2 . Generally this distance can be in the near, intermediate or far-field zone of source radiation. For reception of an objective estimation of the value R_2 it is necessary to know analytical expression for all the electromagnetic field components of informative signals radiation at an arbitrary distance from the technical facilities to the point of observation in the near and intermediate zones of these antennas. Currently the analytical analysis of compromising emanations processes is based on the following principles: 1) radiators are analyzed only in the far-field zone, 2) theoretical models of compromising emanations are based on linear dipole and elementary round frame , 3) electrodynamics in frequency domain is used for calculatins of phase and amplitude characteristics of spurious signals. Thus, now boundaries of R_2 zone are defined conditionally without a sufficient electrodynamic substantiation that is not admissible.

For consistent assessment of spurious radiation it is necessary: 1) to solve outer electrodynamics problem in time domain, 2) to derive the expressions for electromagnetic fields in the near and far field zones as well.

Among methods of the external electrodynamics problem decision it is necessary to note the Evolutionary Approach to Electrodynamics and non-stationary Hertz potentials technique. The Evolutionary Approach to Electrodynamics developed in [12] is oriented on study of the electromagnetic fields in time domain. It means that it is free of the classical presupposing of steady-state time varying of all electromagnetic quantities at a single frequency, by definition. Though approach is oriented on Electrodynamics in time domain, most of the methods of the classical theory widely developed in frequency domain for the monochromatic fields can be nevertheless used directly within the frame of Evolutionary Approach to Electrodynamics proposed.

One more simple method for finding compromising emanations in time domain is non-stationary Hertz potentials technique. Based on this technique the problem of spurious radiation of flat linear source stimulated by the running wave of the current with arbitrary time dependence is considered.

To derive the components for electromagnetic fields, start with the Maxwell's equations in free space in time domain.

And complement the Maxwell's equations of boundedness of field energy:

$$\int_{t_1}^{t_2} dt \int_{z_1}^{z_2} dz \int_0^{2\pi} d\varphi \int_0^{\infty} \rho d\rho \left(\left|\vec{E}\right|^2 + \left|\vec{H}\right|^2 \right) < \infty . \tag{1}$$

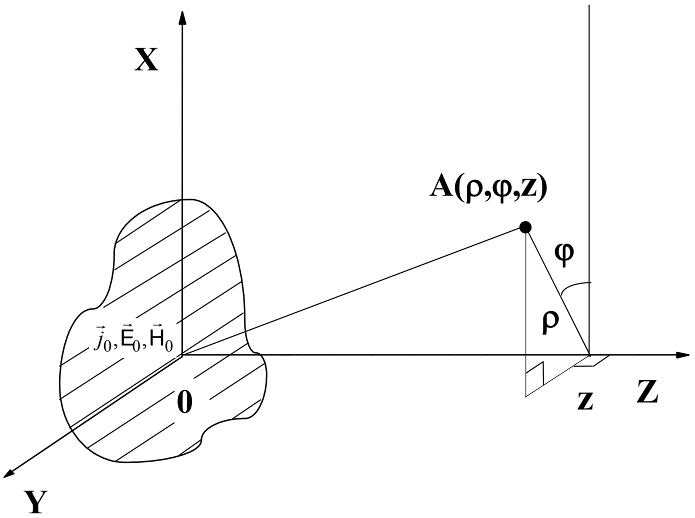


Fig. 3. Geometrical arrangement for finding spurious radiation

For calculating all the component of spurious electromagnetic field it is necessary to know the geometry of the radiator and current distribution along the emitter. As an example we will consider random flat emitter. In general case the fields of flat emitter can be calculated under the following formulas:

$$\vec{A}(p,t) = \frac{\mu_o}{4\pi} \int_V \frac{\vec{I}(t - r/c)}{r} dV , \quad \vec{H} = \frac{1}{\mu_0} rot\vec{A} , \quad \vec{E} = c^2 \int_0^t graddiv\vec{A}\, dt - \frac{\partial \vec{A}}{\partial t} . \tag{2}$$

It is necessary to know the amplitude, phase and polarization characteristics of radiation in the whole space of observation, including the near and intermediate zone of the radiating system. Thus the equations (2) can not be simplified by expansion in a series of small parameter, as is usually done for the calculation of fields in the far field.

The standard design procedure of a field of flat curvilinear radiations looks as follows [13, 14]. The radiator form is set parametrically $x = r(\tau),\ y = r(\tau)$. The arch element on which there is an integration, is equal to

$$dl = \sqrt{\left(\frac{dr}{d\tau} \right)^2 + \left(\frac{ds}{d\tau} \right)^2} . \tag{3}$$

Vector potential in this case is equal to:

$$A_x(p,t) = \frac{\mu_o}{4\pi} \int_\tau \frac{I_x(l, t - R/c)}{R} \dot{r}(\tau) d\tau , A_y(p,t) = \frac{\mu_o}{4\pi} \int_\tau \frac{I_y(l, t - R/c)}{R} \dot{s}(\tau) d\tau . \tag{4}$$

The approach of the given current is used. In the near-field zone of radiation electromagnetic vectors in the Cartesian and Spherical coordinate systems have all 6 components. Given analytical expressions can be used in the field of technical protection of information.

The theory of compromising emanation radiation can be substantially improved by applying time-frequency representations of spurious signals. When it is necessary we propose to use for investigating the structure of the signals with peculiarities such time-frequency representations as: continuous wavelet transform (CWT), discrete wavelet transform (DWT), analytical wavelet transform (AWT), Choi-Williams transform, Wigner transform (WiT), Fourier spectrogram (FS) and Hilbert–Huang transform (HHT) [15-19].

CONCLUSIONS

The problem of compromising radiation of spurious signals in the near, intermediate and far zones of observation in time domain are considered. The goal of the given approach is to speed the development of technical protection of information. The difficulties of System Analysis are connected with bulky mathematical calculations as well as difficulties in the numerical programming. But in its turn using systems of computer mathematics such as MathCAD or Matlab these difficulties can be easily overcome.

The application of the new method allows us to investigate compromising of technical means in time and frequency domain.

REFERENCES

1. Harold Joseph Highland: Electromagnetic Radiation Revisited. Computers & Security, Vol. 5, pp. 85–93 and 181–184, 1986.
2. Harold Joseph Highland: The Tempest over Leaking Computers. Abacus, Vol. 5, No. 2, pp. 10–18 and 53, 1998.
3. Wim van Eck: Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? Computers & Security, Vol. 4, pp. 269–286, 1985.
4. Peter Smulders: The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables. Computers & Security, Vol. 9, pp. 53–58, 1990.
5. Markus G. Kuhn: Optical Time-Domain Eavesdropping Risks of CRT Displays, Proceedings 2002 IEEE Symposium on Security and Privacy, Berkeley, California, 12-15 May 2002, IEEE Computer Society, pp. 3-18, ISBN 0-7695-1543-6.
6. Markus G. Kuhn: Electromagnetic Eavesdropping Risks of Flat-Panel Displays, 4th Workshop on Privacy Enhancing Technologies, 26-28 May 2004, Toronto, Canada, Proceedings, LNCS 3424, pp. 88–105, Springer-Verlag.
7. Markus G. Kuhn: Security Limits for Compromising Emanations. J.R. Rao, B. Sundar (Eds.): Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), 29 August–1 September 2005, Edinburgh, Scotland, LNCS 3659, pp. 265–279.
8. Tanaka Hidema, Takizawa Osamu:A Trial of the Interception of Display Image Using Emanation of Electromagnetic Wave. Journal of the Institute of Image Electronics Engineers of Japan (S0815A), 2005, ISSN:0285-9831, Vol 34; No.2; pp147-155.
9. Martin Vuagnoux, Sylvain Pasini, Compromising Electromagnetic Emanations of Wired and Wireless Keyboards, 18th USENIX Security Symposium (Usenix Security '09), Montreal, Canada, August 10-14, 2009, p. 1-16
10. Asonov D., Agrawal R. Keyboard Acoustic Emanations. In IEEE Symposium on Security and Privacy (2004), IEEE Computer Society, pp. 3-11.
11. Markus G. Kuhn, Ross J. Anderson: Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations, in David Aucsmith (Ed.): Information Hiding, Second International Workshop, IH’98, Portland, Oregon, USA, April 15-17, 1998, Proceedings, LNCS 1525, Springer-Verlag, pp. 124-142, ISBN 3-540-65386-4.
12. Tretyakov O. A. Essentials of Nonstationary and Nonlinear Electromagnetic Field Theory // Hashimoto M., Idemen M., Tretyakov O. A. Analytical and Numerical Methods in Electromagnetic Wave Theory. – Tokyo: Science House Co, Ltd, 1993. – 572 p.
13. Крымский В. В. Антенны несинусоидальных волн. – Челябинск: Изд-во ЦНТИ, 2004. 133 с.
14. Шубарин Ю.В. Антенны сверхвысоких частот. - Х.: Изд. Харьковского гос. университета, 1960. -283 с.
15. The transforms and applications handbook / Editor-in-chief, Alexander Poularikas.- USA: CRC Press, 1996. - 1335 p.
16. О. В. Лазоренко, С. В. Лазоренко, Л. Ф. Черногор. Вейвлет-анализ модельных сверхширокополосных сигналов // Успехи современной радиоэлектроники. – 2006. – №8. – С. 47-61.
17. I. Daubechies. The wavelet transform, time-frequency localization and signal analysis. — IEEE Trans. Inf. Theory, vol. 36 (1990), pp. 961–1005.
18. Wigner E. P. On the quantum correction for thermo-dynamic equilibrium // Phys. Rev. – 1932. – Vol. 40. – P. 749-759.
19. Huang, N.E., Shen, Z., Long, S.R., Wu, M.C., Shih, S.H., Zheng, Q., Tung, C.C., and Liu, H.H., The empirical mode decomposition method and the Hilbert spectrum for non-stationary time series analysis, Proc. Roy. Soc. London, A454, 903-995, 1998.