Analysis of Electromagnetic Emissions for Data Protection

Hapichenko Andrii Mykolaiovych[1],

[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, andrii.hapichenko@nure.ua

Zabolotnyi Volodymyr Illich[2]

[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, volodymyr.zabolotnyi@nure.ua

Abstract. *This paper analyzes stray electromagnetic emissions from the video path of computing devices to assess information leakage risks. A mathematical model using the transfer function evaluates electric and magnetic fields across wide frequency and distance ranges. The results aid in developing effective information protection systems, offering solutions to enhance data security.*

Keywords*: stray electromagnetic emissions; computing devices; transfer function; information security; Maxwell's equations; video path; electromagnetic field.*

I. Introduction and Problem statement

The widespread use of computing devices in critical sectors like government, finance, and healthcare has raised concerns about data leakage through stray electromagnetic emissions (SEME). These parasitic emissions, particularly from the video path, generate high-frequency signals that can be intercepted, forming a technical channel of information leakage (TCIL) [1]. The growing reliance on information technologies amplifies the risk of security breaches. While prior studies have explored electric [2] and magnetic [3] field emissions, a unified model across wide frequency and distance ranges is needed. This work develops a mathematical model using the transfer function to evaluate SEME from the video path, offering novel insights and practical solutions for advanced technical information protection systems.

II. Problem solution and Results

The research methodology uses Maxwell's equations to model stray electromagnetic emissions (SEME) from the video path of computing devices, leveraging established theories [4]. Test patterns of alternating black and white pixels simulate video signals, producing discrete odd harmonics analyzed via Fourier series [2]. The electric field for a loop antenna model is given by:

$$E = \frac{kWsI * \sin\theta}{4\pi r} \quad (1)$$

where k – wave number (k = 2πf / c, f is frequency, c is speed of light); W – wave impedance (120π Ω); s – loop area; I – harmonic current amplitude; θ – meridional angle; r – distance.

The transfer function:

$$K_{\alpha}^{E}(\omega) = \frac{E_{\alpha}}{I} \quad (2)$$

quantifies emission levels. The magnetic field is modeled using Maxwell's second equation, capturing fields from moving charges and varying electric fields [3]. Analysis spans 0.1–1000 MHz and 0.1–100 meters, covering near, intermediate, and far zones [1]. Results show emission strength varies with frequency and distance, with higher risks at higher frequencies and shorter distances. The magnetic field significantly impacts near-field zones, informing protection norms [3]. The model supports extrapolation from measurements, aligning with security standards, and was validated theoretically. It aids in designing countermeasures like shielding and signal suppression to reduce TCIL risks.

III. Conclusions

The developed mathematical model offers a robust framework for analyzing stray electromagnetic emissions from computing devices, integrating electric and magnetic field components to evaluate and mitigate information leakage risks. The transfer function effectively quantifies emission behavior, highlighting key frequency and distance dependencies critical for protection measures [2]. The study confirms the video path's vulnerability to interception, emphasizing the need to assess both field components [3]. By enabling extrapolation of emission levels from measurements, the model supports targeted countermeasures like advanced shielding and signal suppression [1]. Its novelty lies in unifying prior findings into a comprehensive framework with practical applications. Future work will explore environmental factors and adaptive protection strategies for dynamic threats.

References

[1] S. O. Ivanchenko, O. V. Havrylenko, O. A. Lypskyi, A. S. Shevtsov, "Technical channels of information leakage. Procedure for creating technical information protection systems," Kyiv: NTUU "KPI," 2016, 101 p.

[2] V. I. Zabolotnyi, Ye. V. Herasymenko, V. I. Perepadia, "Study of signal shape changes in the channel of stray electromagnetic emissions of a monitor," Radio Engineering, Kharkiv, vol. 176, pp. 116–121, 2014.

[3] V. V. Pilinskyi, "Technical electrodynamics and radio wave propagation," Kyiv: NTUU "KPI," 2014, 336 p.

[4] J. Clerk Maxwell, "A treatise on electricity and magnetism," 3rd ed., vol. 2, Oxford: Clarendon, 1892, pp. 68–73.

[5] M. Young, "The technical writer's handbook," Mill Valley, CA: University Science, 1989.