# AN IMPROVED APPROACH TO PROTECTING VIDEO PATHS OF COMPUTER SYSTEMS FROM INFORMATION LEAKAGE VIA CHANNELS OF SPURIOUS ELECTROMAGNETIC EMISSIONS

**Foziljonov Kh.I.**

*Tashkent University of Information Technologies named after Muhammad al-Khwarizmi*

*E-mail: foziljonov.x.i@gmail.com*

**Abstract.** This paper proposes an improved method for actively masking spurious electromagnetic emissions (SEME) from computer system video paths. This method generates targeted masking interference using the video path clock signal as a carrier and a nonlinear transformation of the sum of the clock and noise components. This approach ensures that the spectral structure of the masking effect is matched to the harmonic component of the SEME by automatically adjusting the frequency parameters of the interference when the video path operating mode changes. A step-by-step scheme for generating a masking signal is described. It is focused on the spectral-temporal overlap of the synchronization and information components of the SEME, which complicates the restoration of video signal parameters on the side of a potential intruder.

**Keywords:** Spurious electromagnetic emissions, computer system video path, targeted masking interference, clock signal as a carrier, automatic frequency agility, nonlinear transformation; spectral-temporal overlap, information security.

**Аннотация.** В работе предложен усовершенствованный метод активного маскирования побочных электромагнитных излучений (ПЭМИ) видеотрактов компьютерных систем, основанный на формировании прицельной маскирующей помехи с использованием тактового сигнала видеотракта в качестве несущей и нелинейного преобразования суммы тактовой и шумовой составляющих. Подход обеспечивает согласование спектральной структуры маскирующего воздействия с гармонической составляющий ПЭМИ за счёт автоматической перестройки частотных параметров помехи при изменении режима работы видеотракта. Описана поэтапная схема формирования маскирующего сигнала, ориентированная на спектрально-временное перекрытие синхронизационных и информативных компонент ПЭМИ, что затрудняет восстановление параметров видеосигнала на стороне потенциального нарушителя.

**Ключевые слова:** Побочные электромагнитные излучения, видеотракт компьютерных систем, прицельная маскирующая помеха, тактовый сигнал как несущая, автоматическая перестройка частоты, нелинейное преобразование; спектрально-временное перекрытие, защита информации.



ISSN 3030-3907

**Annotatsiya.** Mazkur ishda kompyuter tizimlari videotraktlarining yon elektromagnit nurlanishlarini (YEN) faol niqoblashning takomillashtirilgan usuli taklif etiladi. Ushbu usul videotraktning takt signalidan tashuvchi sifatida foydalanish hamda taktli va shovqinli tarkibiy qismlar yig‘indisini nochiziqli o‘zgartirish asosida yo‘naltirilgan niqoblovchi xalaqitni shakllantirishga asoslanadi. Yondashuv videotrakt ish rejimi o‘zgarganda xalaqitning chastota parametrlarini avtomatik qayta sozlash orqali niqoblovchi ta’sirning spektral tuzilmasini YEMNning garmonik tarkibi bilan moslashishini ta’minlaydi. Niqoblovchi signalni shakllantirishning bosqichma-bosqich tavsiflangan bo‘lib, u YENning sinxronizatsion va axborot komponentlarini spektral-vaqt bo‘yicha qoplashga yo‘naltirilgan, bu esa potentsial axborotni ushlab oluvchi tomonida videosignal parametrlarini tiklashni murakkablashtiradi.

**Kalit so‘zlar.** Yon elektromagnit nurlanishlar; kompyuter tizimlari videotrakti; yo‘naltirilgan maskalovchi halaqit; taktli signal tashuvchi sifatida; chastotani avtomatik qayta sozlash; nolinear o‘zgartirish; spektral-vaqt bo‘yicha niqoblash; axborotni himoyalash

## INTRODUCTION

With the widespread use of computer systems (CS) and digital display devices, the problem of protecting confidential data from leakage via spurious electromagnetic radiation remains highly relevant [1-4]. Computer system video paths are among the most vulnerable elements in terms of information compromise, as the generated video signals possess a distinct structure, high periodicity, and spectral localization, which significantly simplifies their interception and subsequent recovery [2, 4-5].

Existing methods for active SEME masking are typically based on the use of interference with fixed parameters or broadband noise [6-8]. However, such approaches have several limitations: the fixed frequency of the masking interference can be compensated or filtered through targeted interception using adaptive spectral and temporal analysis methods, while broadband noise requires significant energy expenditure and can lead to unwanted electromagnetic interference for electronic devices [9].

Despite the availability of technical solutions and scientific research aimed at protecting information from leakage through electromagnetic channels, the problem of increasing the efficiency and adaptability of methods for masking video paths of computer systems in a changing electromagnetic environment remains relevant and requires further research [9-10].

## METHODS



ISSN 3030-3907

The methodological basis of the study is formed on the basis of an analysis of existing devices, scientific literature and patent sources dedicated to the protection of computer systems from information leakage through channels of side electromagnetic radiation [11-15].

The paper [11; pp. 55–56] presents software-defined radio (SDR)-based devices that employ modulation schemes on multiple carrier frequencies. An SDR device generates at least two signals: the first signal covers the SEME frequency band, and the second is a pseudo-signal that serves as a false signal for the interceptor's receiver. The disadvantage of this approach is that the generated interference masks only one harmonic component of the information signal.

In [12; pp. 132–137], a mobile interference generator was developed that connects to a personal computer via a VGA interface. Masking interference is generated based on signals from the computer's video interface. A significant drawback of this device is its low efficiency, due to differences in the temporal and frequency structure of VGA interface signals and modern digital video interfaces such as DVI and HDMI.

A mobile interference generator powered by a computer's USB port and incorporating multiple electromagnetic interference sources is proposed in [13; pp. 35–36]. The device generates a broadband noise signal. Its disadvantages include uneven spectral power density of the noise signal, the inability to adjust output power, and reduced efficiency when individual amplifying elements fail.

A method for protecting an information processing system from stray electromagnetic radiation, a device for implementing the method, and a noise signal generator for implementing the device [14], which is a hardware module that generates a masking noise signal and superimposes it on the SEME of a video path. Analysis showed that in the proposed method, using the computer system's clock signal as a carrier results in the spectrum overlapping with only one harmonic component of the information signal, and the device's connection method requires additional matching devices.

A device for protecting automated systems from information leakage via SEME channels [15] is also known. It is implemented as a modular system using a spectrum analyzer. In the proposed approach, the signal from the spectrum analyzer's internal oscillator is used as the carrier. Disadvantages of this device include high complexity and cost, the need for manual configuration, operator involvement in the SEME spectrum analysis process, and the lack of ability to adjust the amplifier cutoff angle, which reduces the effectiveness of suppressing individual information-rich harmonic components.

## RESULTS



ISSN 3030-3907

The conducted methodological analysis shows that methods [14] and [15] have a higher potential efficiency compared to devices [11-15], however, the identified limitations necessitate their further improvement.

In this regard, it is proposed to improve the method [14] for masking signals of side electromagnetic emissions from video paths of computer systems, based on automatic frequency tuning of the masking interference.

The proposed improved method is based on the introduction of targeted masking interference into the area of formation of informative harmonics of the SEME of the CS video path - *Q(t)*, which mask the informative harmonics of the SEME of the CS video path (Fig. 1).

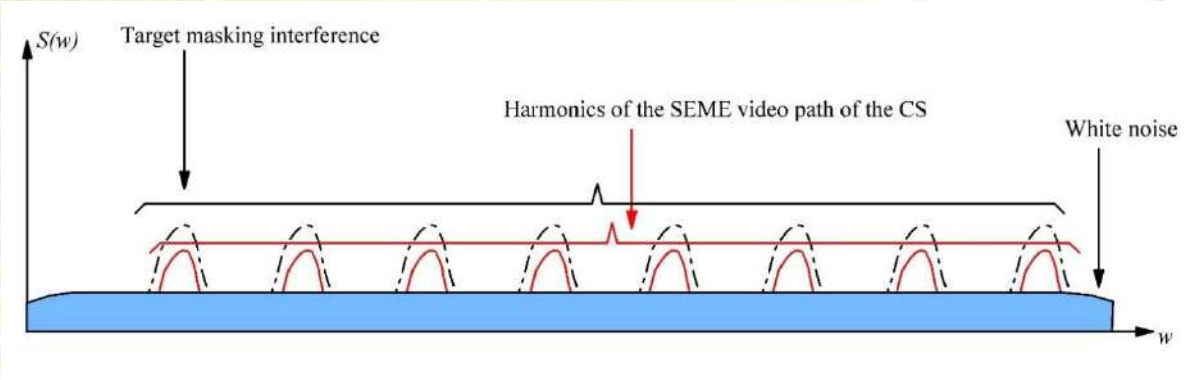



**Fig. 1. Masking of SEME signals with targeted interference**

The targeted masking interference itself is generated by detecting the nonlinear transformation of the sum of two signals: a clock signal and a noise signal. Furthermore, the frequency of the targeted masking interference automatically changes with the frequency of the clock signal in the computer's video path.

The generated signal is emitted into the air, creating an additional electromagnetic field in the frequency domain that overlaps with the information-bearing harmonics of the SEME in the computer's video path. As a result, the spectral components of the targeted masking interference overlap the spectral components of the SEME in the computer's video path.

As a result of superposition of the masking signal on the TEM video path, masking of informative spectral and temporal components occurs, which disrupts the possibility of stable extraction of the SEME signal from the video path and makes restoration of the video frame structure impossible.

The implementation of the method includes four stages (Fig. 2).



ISSN 3030-3907

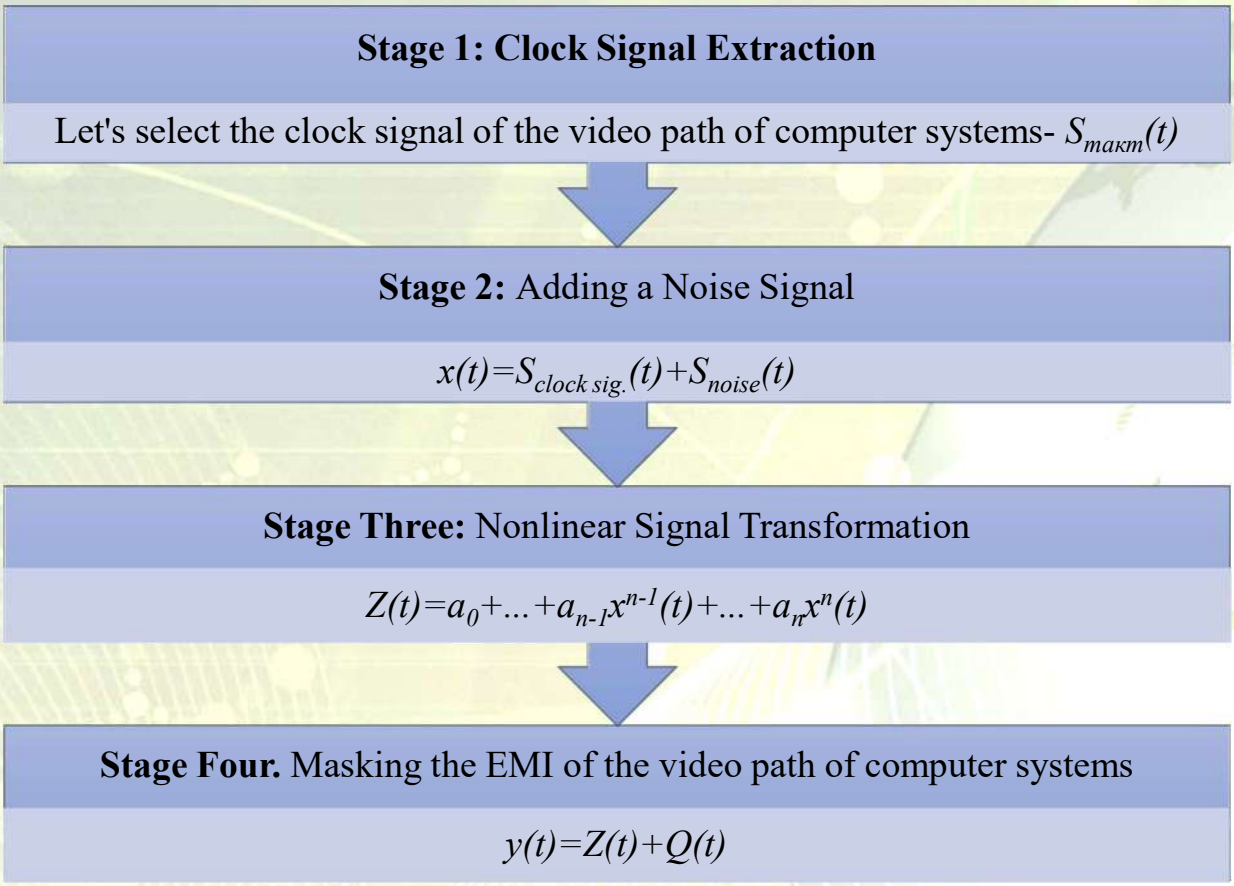



**Fig. 2. Block diagram of the implementation of the method for masking the EMIS of video paths of computer systems with targeted interference**

**Stage I. Extraction of the video signal clock.** At this stage, the clock signal is extracted from the SVT video path. This is because the clock signal is the carrier signal. Furthermore, extracting the clock signal enables automatic frequency tuning of the masking interference.

**Stage II. Adding a noise signal.** The extracted clock signal from the SVT video path is summed with the noise signal.

$$x(t)=S_{clock\ sig.}(t)+S_{noise}(t)$$

**Stage III. Nonlinear signal transformation.** A nonlinear transformation of the signal x(t) is performed using a polynomial approximation:

$$Z(t) = a_0 + ... + a_{n-1}x^{n-1}(t) + ... + a_nx^n(t)$$

where n is the degree of approximation

After nonlinear transformation, additional spectral components are formed, which in the frequency domain will mask the informative harmonics of the video path of the computer system.

**Stage IV. Masking the SEME of the computer equipment's video path.** The generated targeted masking interference is transmitted into the air, creating an additional electromagnetic field in the area where the computer equipment's video path generates spurious electromagnetic emissions.



ISSN 3030-3907

$$y(t) = Z(t) + Q(t)$$

Due to the spectral-temporal overlap of both the synchronization and information components of the SEME by the targeted masking interference, it becomes impossible to reliably isolate the parameters of the temporal structure of the video signal and restore the information content of the image on the receiving side, which leads to a disruption of the process of restoring the video frame.

**DISCUSSION**

The proposed improved method differs from known solutions [11-15] by using the video signal's clock as the carrier and synchronization parameter for generating masking interference, which ensures that its spectral structure is matched to the harmonic organization of the electromagnetic field. This approach enables targeted spectral-temporal overlap of both synchronization and information components of the video signal, unlike methods based on broadband noise or fixed interference parameters.

The use of a nonlinear transformation of the sum of the clock and noise components expands the spectral range of the masking effect by generating combinational and spurious harmonic components. This reduces the possibility of reliably identifying individual harmonics used to reconstruct the temporal structure of the video signal and increases the resilience of the protection system to spectral analysis and synchronization methods.

Prospects for further research include the development of a simulation model, hardware implementation of the method, and the implementation of adaptive mechanisms for automatically adjusting masking interference parameters in real time depending on the video signal operating mode and the electromagnetic environment.

**CONCLUSION**

This paper presents an improved method for targeted masking of spurious electromagnetic emissions from computer system video paths. This method utilizes a clock signal as a carrier and synchronization parameter, as well as a nonlinear transformation of the sum of the clock and noise components. The proposed step-by-step scheme for generating a masking signal ensures spectral and temporal overlap of the synchronization and information components of the SEME, complicating the reconstruction of video signal parameters on the side of a potential intruder.

The practical significance of this method lies in its ability to be integrated into existing active information security systems without significantly altering the video path architecture.



ISSN 3030-3907

## REFERENCES:

1. Liu, T., & Li, Y. (2019). Electromagnetic Information Leakage and Countermeasure Technique: Translated by Liu Jinming, Liu Ying, Zhang Zidong, Liu Tao. Springer.
2. Хорев, А. А. (2010). Технические каналы утечки информации, обрабатываемой средствами вычислительной техники. Специальная техника, (2), 39-57.
3. Ogli, F. K. I. (2021, November). Study of the spectrum of side electromagnetic radiations of video interface DVI. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-3). IEEE.
4. Kuhn, M. G. (2003).Compromising emanations: eavesdropping risks of computer displays(No. UCAM-CL-TR-577). University of Cambridge, Computer Laboratory.
5. de Meulemeester, P., Scheers, B., & Vandenbosch, G. A. (2020, July). Eavesdropping a (ultra-) high-definition video display from an 80 meter distance under realistic circumstances. In 2020 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI) (pp. 517-522). IEEE.
6. Lavaud C. et al. Whispering devices: A survey on how side-channels lead to compromised information //Journal of Hardware and Systems Security. –2021. –T. 5. –C. 143-168.
7. Guri M., Elovici Y. Bridgeware: The air-gap malware //Communications of the ACM. – 2018. – T. 61. – №. 4. – C. 74-82.
8. Foziljonov, K., & Faziljanov, I. (2023). Active methods and means of information protection against leakage through channels of side electromagnetic radiation and interference. Science and innovation, 2(A4), 46-52.
9. Foziljonov, K. (2025). Analysis of new methods of information protection from the leakage of side electromagnetic radiation from video tract of computer equipment. In Proceedings of the 10th International Scientific and Practical Conference “Scientific Community: Interdisciplinary Research” (pp. 276–279). Hamburg, Germany.
10. Фазилжанов, И. Р., & Фозилжонов, Х. И. (2023). Исследование зависимости вероятности ошибки оптимального когерентного разведовательного приемника при перехвате пэми видеотракта компьютеров от ложной тактовой синхронизации. Science and innovation, 2(Special Issue 3), 411-414.
11. Yao K., Lan S., Xia M., Chen L. Active countermeasure using EMI honeypot against TEMPEST eavesdropping in high-speed signalling // 2018 USNC-URSI



ISSN 3030-3907

Radio Science Meeting (Joint with AP-S Symposium). — Boston, 2018. — p. 55–56.
12. Suzuki Y., Akiyama Y. Jamming technique to prevent information leakage caused by unintentional emissions of PC video signals // 2010 IEEE International Symposium on Electromagnetic Compatibility. — Fort Lauderdale, 2010. — p. 132–137.
13. Жалковский М. В., Сидоренко А. В. Мобильный генератор электромагнитного шума с питанием от порта USB //Электроника инфо. – 2013. – №. 6. – С. 35-36.
14. Патент РФ RU 2493594 от 20.09.2013г., C2 G06F 21/00, H04K 3/00. Лепеха Ю. П. Способ защиты обрабатываемой информации средствами вычислительной техники путем зашумления информативных побочных электромагнитных излучений и наводок, устройство защиты информации для реализации способа
15. Патент РФ RU 2421917 от 20.00.2011г., C1 H04K 1/04, H03B 29/00. Дёмин В. М., Лепеха Ю. П., Поярков Л. А. Способ защиты системы обработки информации от побочных электромагнитных излучений, устройство для реализации способа и генератор шумового сигнала для реализации устройства.


ISSN 3030-3907