

ДОСЛІДЖЕННЯ ПАРАМЕТРІВ СПЕКТРІВ ТА СИГНАЛІВ ВІД ПРИБОРІВ ТА ІНТЕРФЕЙСІВ АВТОМАТИЗОВАНИХ СИСТЕМ

І. О. Пахнюк^{1,а}, В. М. Бездітний^{1,2}, Є. А. Зайцев^{1,2}

¹ Навчально-науковий Фізико-технічний інститут

² НДЦ «ТЕЗІС»

Анотація

У роботі досліджено проблему технічного витоку інформації через електромагнітне випромінювання (ЕМВ), що виникає внаслідок побічного випромінювання пристроїв автоматизованих систем. Проведено теоретичний аналіз фізичних принципів формування ЕМВ та його здатності передавати конфіденційну інформацію. Виконано класифікацію потенційних джерел витоку за типом пристрою, режимом роботи та конструктивними характеристиками.

Увагу зосереджено на зонах підвищеної ймовірності витоку з урахуванням просторового розміщення, заземлення та типів інтерфейсів. Розглянуто методи аналізу сигналів (спектральні, фільтраційні) і технічні засоби зменшення побічного ЕМВ. Узагальнено підходи до зниження витоків через екранування, фільтрацію живлення, вдосконалення схемотехніки та організаційні заходи.

Результати можуть бути використані при проектуванні захищених автоматизованих систем і формуванні технічних вимог до їх інформаційної безпеки.

Ключові слова: електромагнітний витік, побічне випромінювання, технічний захист інформації, спектральний аналіз, автоматизовані системи.

Вступ

Електромагнітне випромінювання, що виникає при коливаннях електричних і магнітних полів, може ненавмисно генеруватися електронними пристроями та поширюватися в середовище. За певних умов воно несе інформацію про оброблювані сигнали, утворюючи побічні канали витоку конфіденційних даних. Дослідження показали можливість зчитування інформації з дисплеїв, клавіатур, ліній живлення, мікропроцесорів та інших елементів. З розвитком спектрального аналізу зростає актуальність вивчення таких витоків і методів їх мінімізації.

1. Теоретичні засади електромагнітних витоків інформації

Електромагнітне випромінювання є невід'ємним супутником роботи електронних пристроїв, що функціонують в автоматизованих системах. Це випромінювання, яке часто називають побічним (ПЕМВ), може стати каналом витоку конфіденційної інформації, навіть без фізичного доступу до технічних засобів обробки даних [1].

Фізично ПЕМВ виникає внаслідок струмів, що протікають провідниками, перемикань транзисторів, змін електричних та магнітних полів. Залежно

від характеристик пристрою, частоти, типу сигналів та навантаження, спектр випромінювання може містити інформативні компоненти, які корелюють із оброблюваними даними. Це робить можливим перехоплення та реконструкцію інформації шляхом аналізу електромагнітного фону, що супроводжує роботу пристрою.

До основних джерел ПЕМВ в автоматизованих системах належать:

- **Монітори** [2] – особливо з електронно-променевою трубкою (CRT), а також сучасні РК-екрани;
- **Клавіатури** [3, 4] — завдяки різному електромагнітному профілю натискання клавіш;
- **Принтери** [5, 6] — під час формування зображення, особливо лазерні;
- **Процесори та шини даних** — внаслідок активної обробки інформації;
- **Комутаційні інтерфейси** (USB, HDMI, Ethernet) — які можуть випромінювати сигнали, що містять інформативні складові.

Атаки на основі ПЕМВ включають:

- **Пасивне перехоплення** — аналіз спектру без активного втручання;
- **Аналіз екранного відображення** — реконструкція зображення, яке виводиться на монітор;
- **Аналіз натискань клавіш** — визначення вве-

^аillpah-ipt25@iit.kpi.ua

дених символів за характерними сигналами;

- **Аналіз активності інтерфейсів** — визначення оброблюваних даних через ЕМІ, створювані портами.

Для протидії електромагнітним витокам використовуються стандарти та рекомендації, такі як TEMPEST (США) [7], що визначають рівні допустимих випромінювань і методи їх екранізації. Застосовуються активні й пасивні засоби захисту: металеве екранування, фільтрація живлення, архітектурні заходи, розведення сигнальних трас, а також криптографічні методи як додатковий бар'єр.

2. Практичне дослідження побічних електромагнітних випромінювань

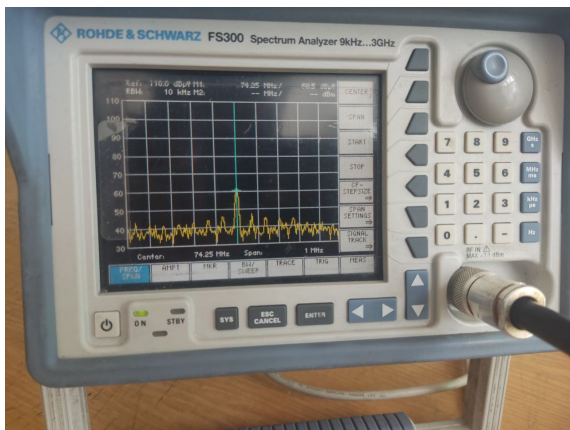


Рис. 1. Спектроаналізатор



Рис. 2. Лабораторне устаткування

З метою оцінки потенційної загрози електромагнітного витоку інформації було проведено експериментальне дослідження побічних випромінювань, що генеруються елементами персонального комп'ютера. Основна увага приділялася сигналам, що випромінюються монітором та USB-інтерфейсами.

Для вимірювань використовувалося спеціалізоване приймальне обладнання з направленими та широкопосмуговими антенами. Дані фіксувалися на різних відстанях (від 0,5 до 3,5 метрів) до джерела ПЕМВ. Сигнали оброблялися за допомогою спектроаналі-

затора та програмного забезпечення, що дозволяло проводити детальний спектральний аналіз.

Було виявлено, що на відстані до 3 метрів можна виділити окремі компоненти, пов'язані із зміною зображення на екрані або передачею даних через USB. Це підтверджує наявність вразливих каналів витоку інформації через ПЕМВ.

Отримані результати можуть бути використані для оцінювання ризиків у реальних інформаційних системах та розробки рекомендацій щодо вдосконалення систем технічного захисту. Також вони слугують базою для розробки детекторів побічного випромінювання та систем раннього виявлення загроз.

2.1. Лабораторне обладнання

Таблиця 1. Лабораторне обладнання для дослідження ПЕМВ

Обладнання	Характеристика
Монітор Acer SA240Ybid	Роздільна здатність: 1920x1080 (Full HD)
	Частота оновлення: до 75 Гц
	Тип панелі: IPS
Антенна ЕМА-2000	Широкопосмугова антена
	Підтримує вимірювання на різних частотах 0,009...2000 МГц
	Коефіцієнт калібровки антени 25 дБ (± 6 дБ)
Спектроаналізатор FS300	Частотний діапазон: 9 кГц – 3 ГГц
	Роздільна здатність: 1 Гц
	Ширина смуги пропускання: від 200 Гц до 1 МГц
	Максимальний вхідний рівень: до +33 дБм

2.2. Методика вимірювання

- Використання ЕМА-2000 для збору сигналів на різних відстанях (від 0,5 до 3,5 м).
- Обробка зібраних даних за допомогою спектроаналізатора FS300.
- Аналіз гармонік, зокрема першої, як найбільш інформативної.
- Визначення рівня шуму та порівняння його з рівнем сигналу для виявлення можливих витоків.

2.3. Теоретичне обґрунтування експерименту

Експеримент з виявлення можливих каналів витоку інформації через побічні електромагнітні випромінювання (ПЕМВ) ґрунтується на аналізі високочастотних сигналів, які можуть утворюватися в процесі роботи електронних компонентів персонального комп'ютера. В основі дослідження лежить теоретичне припущення, що інформаційні процеси

в електронних пристроях супроводжуються ПЕМВ, які можуть частково відображати зміст оброблюваних даних.

Основну увагу було приділено гармонічному аналізу сигналів. Перша гармоніка розглядалася як найбільш інформативна, оскільки вона зазвичай характеризується найвищою амплітудою та мінімальними спотвореннями.

Для оцінки інформативності сигналів залежно від відстані до джерела було передбачено збір спектральних даних з різної відстані. Це дозволило простежити закономірність зміни потужності сигналу при віддаленні приймальної антени, а також визначити, які гармоніки залишаються помітними на різних дистанціях.

Крім того, передбачалося вимірювання рівня шуму в лабораторному середовищі з метою подальшого порівняння його з рівнем сигналів. Це необхідно для встановлення мінімального порогового рівня, нижче якого неможливо виділити інформативні компоненти без застосування додаткових методів фільтрації чи обробки сигналів.

Таблиця 2. Результати вимірювань для монітора та USB 2.0

Елемент	Відстань (м)	Рівень сигналу (дБ)
Монітор 1-ша гармоніка	0,5	61 дБ
	1	56,9 дБ
	1,5	53,5 дБ
	2	45,8 дБ
	2,5	43,4 дБ
	3	41 дБ
	3,5	37 дБ
Монітор 2-га гармоніка	Безпосередня близькість	37 дБ
Монітор 3-тя гармоніка	Безпосередня близькість	45,2 дБ
ЮСБ 2.0	0,5	47 дБ

Висновки

Емісія електромагнітних хвиль є невід'ємною частиною роботи електронних пристроїв, яка може створювати загрозу несанкціонованого доступу до автоматизованих систем. Первісна орієнтація на технічну ефективність призвела до недооцінки загроз, пов'язаних з витоками інформації через електромагнітне випромінювання. З часом стало зрозуміло, що такі витоки можуть використовуватись для перехоплення даних.

Надійність і безпека систем потребують контролю

за характеристиками сигналів і обмеженням витоків. Тому актуальним є використання захисних технологій — шифрування, фільтрації сигналів, екранування — для протидії зовнішнім загрозам. У зв'язку з ростом кількості атак і вдосконаленням засобів їх реалізації, дослідження електромагнітних проявів пристроїв набуває ключового значення для інформаційної безпеки.

Перелік використаних джерел

1. Identification of Multi-dimensional Electromagnetic Information Leakage Using CNN / J. Mao, P. Liu, J. Liu, S. Shi // IEEE Access. — 2019. — Т. 7. — С. 145714—145724. — DOI: [10.1109/ACCESS.2019.2945812](https://doi.org/10.1109/ACCESS.2019.2945812). — URL: <https://ieeexplore.ieee.org/document/8854058>.
2. Method of Colors and Secure Fonts Used for Source Shaping of Valuable Emissions from Projector in Electromagnetic Eavesdropping Process / A. Boitan, I. Kubiak, S. Halunga, A. Przybysz, A. Stańczak // Symmetry. — 2020. — Т. 12, № 11. — С. 1908. — DOI: [10.3390/sym12111908](https://doi.org/10.3390/sym12111908). — URL: <https://www.mdpi.com/2073-8994/12/11/1908>.
3. A Signal-Denoising Method for Electromagnetic Leakage from USB Keyboards / Y. Peng, J. Zhang, J. Mao, M. Cui // Electronics. — 2023. — Т. 12, № 17. — С. 3647. — DOI: [10.3390/electronics12173647](https://doi.org/10.3390/electronics12173647). — URL: <https://www.mdpi.com/2079-9292/12/17/3647>.
4. Vuagnoux M., Pasini S. Compromising Electromagnetic Emanations of Wired and Wireless Keyboards // Proceedings of the 18th USENIX Security Symposium. — 2009. — С. 1—16. — URL: https://www.usenix.org/legacy/event/sec09/tech/full_papers/vuagnoux.pdf.
5. Kubiak I. Laser Printer as a Source of Sensitive Emissions // Turkish Journal of Electrical Engineering and Computer Sciences. — 2018. — Т. 26, № 3. — С. 1327—1336. — DOI: [10.3906/elk-1705-108](https://doi.org/10.3906/elk-1705-108). — URL: <https://journals.tubitak.gov.tr/elektrik/vol26/iss3/19/>.
6. Kubiak I., Loughry J. LED Arrays of Laser Printers as Valuable Sources of Electromagnetic Waves for Acquisition of Graphic Data // Electronics. — 2019. — Т. 8, № 10. — С. 1078. — DOI: [10.3390/electronics8101078](https://doi.org/10.3390/electronics8101078). — URL: <https://www.mdpi.com/2079-9292/8/10/1078>.
7. Kubiak I., Boitan A., Halunga S. Assessing the Security of TEMPEST Fonts against Electromagnetic Eavesdropping by Using Different Specialized Receivers // Applied Sciences. — 2020. — Т. 10, № 8. — С. 2828. — DOI: [10.3390/app10082828](https://doi.org/10.3390/app10082828). — URL: <https://www.mdpi.com/2076-3417/10/8/2828>.