УДК 004.89:004.056

ЗАГРОЗА ВИКОРИСТАННЯ ШІ ПРИ ПЕРЕХОПЛЕННІ ПЕМВ МОНІТОРА

Попова А. О., Ярмола А.В.
e-mail:anna.popova@nure.ua
Науковий керівник –доцент Ликов Ю.В.
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ
м. Харків, Україна

This study explores the use of artificial intelligence to detect and analyze electromagnetic emissions (EME) from monitors. By applying deep learning techniques, the proposed approach improves image reconstruction accuracy, helping to identify threats and reduce the risk of information leakage. Experimental results show significant improvements in detecting and restoring screen images from EME signals. The research also considers countermeasures and ways to minimize the risks associated with such attacks.

Сучасні методи та системи кібер та інформаційної безпеки стикаються з новими загрозами, пов’язаними з використанням штучного інтелекту (ШІ). Однією з таких загроз є можливість перехоплення побічного електромагнітного випромінювання (ПЕМВ) моніторів для відтворення зображення на екрані. Автоматизовані методи аналізу на базі ШІ можуть підвищити точність і швидкість декодування перехоплених сигналів, збільшуючи таким чином потенційний ризик витоку конфіденційної інформації. Відповідно до досліджень [1-3], навіть невеликі витоки ПЕМВ можуть призвести до суттєвих компрометацій інформації, особливо для пристроїв з телевізійною розгорткою.

Основною проблемою є низька точність існуючих методів декодування сигналів через значний рівень шуму та завад, а також складність у відтворенні візуальної інформації, що обумовлюється сучасними відео інтерфейсами (DVI, HDMI, DP тощо). Основними джерелами ПЕМВ є інтерфейсні відеокабелі, шлейфи, та кола відеопідсилювачів моніторів Завдання дослідження полягає у розробці математичної моделі, яка з урахуванням особливостей ПЕМВ та використанням нейромережевих методів дозволить ефективно реконструювати зображення, підвищуючи якість розпізнавання текстової інформації, що виводиться на екран. Також аналізується вплив характеристик монітора, типу підключення на рівень ПЕМВ.

Для вирішення проблеми пропонується використання алгоритмів глибокого навчання. На першому етапі передбачається збір і аналіз експериментальних даних ПЕМВ від TFT і CRT моніторів. Далі проводиться попередня обробка сигналу для зменшення шуму та виділення найбільш інформативних спектральних компонентів. Застосування нейронної мережі буде включати згорткові та рекурентні шари, що дозволить обробляти сигнали у часовій та частотній областях. Навчання моделі відбуватиметься на

великій вибірці даних із використанням технік розширення датасету для покращення генералізації. Передбачено порівняння різних архітектур мереж для визначення найбільш ефективної структури, а також оптимізація гіперпараметрів для підвищення точності реконструкції зображень. Особливу увагу приділено створенню методів адаптивної фільтрації шуму та відновленню дрібних деталей зображень, що значно покращить точність реконструкції.

Результати дослідження дають змогу оцінити ефективність застосування ШІ для розшифрування ПЕМВ та визначити оптимальні методи їх обробки. Досліджено вплив рівня шуму та характеристик моніторів на якість відтворення інформації. Окрім того, експериментальне дослідження допоможе виявити основні джерела ПЕМВ у відеотракті ПК, що сприятиме розробці ефективних заходів захисту, таких як екранування або фільтрація сигналів.

Окремо в роботі досліджено можливість інтеграції запропонованих методів захисту у системи безпеки.

Результатом роботи є підтвердження того, наскільки реальною є загроза використання ШІ для перехоплення інформації через ПЕМВ монітора, та надають рекомендації щодо методів протидії. Запропоновані алгоритми можуть суттєво покращити точність декодування сигналів, що створює нові виклики для інформаційної безпеки. Висновки цього дослідження сприяють розробці нових стратегій захисту конфіденційної інформації та покращенню рівня безпеки інформаційних систем.

Список використаних джерел:

1. Deep-TEMPEST: Using Deep Learning to Eavesdrop on HDMI from its Unintended Electromagnetic Emanations URL: https://arxiv.org/html/2407.09717v1 (дата звернення: 20.02.2025).

2. Information Leakage from Optical Emanations URL: https://arxiv.org/pdf/2307.07043 (дата звернення: 15.02.2025).

3. Лыков, Ю. В. Концепция построения защищенных видеосистем / Ю. В. Лыков, О. А. Сягаева // Радиотехника : Всеукр. межвед. науч.-техн. сб. – Харьков, 2013. – Вып. 173. – С. 208 – 215.