УДК 621.395.7 (043.2)

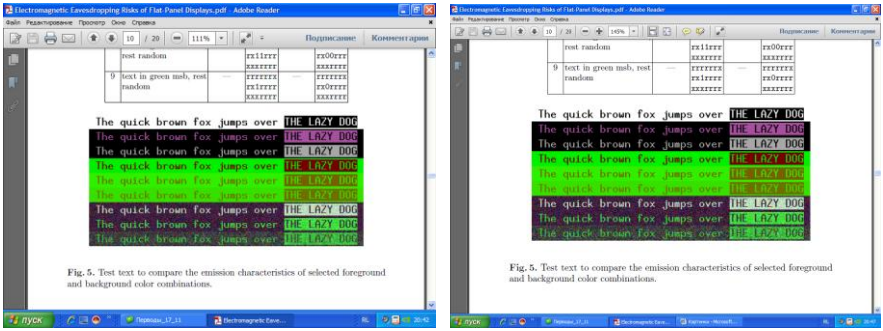
Д.В. Євграфов, Ю.Є Яремчук
Вінницький національний
технічний університет, м. Винниця

ОЦІНЮВАННЯ РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ПАСИВНИХ АЛГОРИТМІЧНИХ МЕТОДІВ ПРОТИДІЇ ЇЇ ВИТОКУ З ЕКРАНІВ МОНІТОРІВ

Крім давно відомих пасивних методів захисту інформації від витоку з екранів працюючих моніторів, пов'язаних з технологіями Low radiation та створенням додаткових екранів перед монітором і екрануванням монітору с заду, а також екрануванням сигнальних кабелів та інших вводів у монітор, очевидним стає підвищення ймовірності «перехоплення» зображення за допомогою спеціалізованого технічного засобу розвідки противника (СТЗРП) зі зростанням співвідношення часу накопичення сигналу до періоду кадрової розгортки незмінного зображення на екрані монітору – $T_{\text{а}}/T_{\text{к}}$.

Це співвідношення збільшується зі збільшенням часу аналізу $T_{\text{а}}$ незмінного зображення на екрані монітору. Зрозуміло, що коли йдеться, наприклад, про набір якогось тексту конфіденційної інформації у текстовому редакторі Word її витік стає більш можливим, наприклад, коли заповнюються останні строки на сторінці. У цьому випадку більша частина сторінки вже містить незмінну на даний момент інформацію, і лише незначна нижня частина сторінки заповнюється та має змінний характер.

Більшість моніторів мають однакові значення частоти кадрової розгортки $f_{ver} = 1/T_{\text{к}}$ для більшості типів програмного забезпечення (ПЗ). Це досягається уніфікацією ПЗ під різні типи драйверів для комплектуючих. Проте, як це було зроблено у старих типах моніторів, властивості екрану можуть бути зміненими. На рис. 1 подано зображення екранів моніторів для різних режимів роботи його відео карти з однаковим фрагментом тексту відомої статті Маркуса Куна [1], в якій він уперше дослідив витік інформації з моніторів на рідинно-кришталевих структурах. Саме з виходом друком цієї роботи почалися серйозні світові дослідження у галузі витоку інформації з екранів сучасних моніторів.



а) *б*)

Рис. 1. Вигляд екрану монітору: *а*) для режиму SVGA, 800×600, $f_{ver}=60{,}3$ Гц; *б*) для режиму SXGA, 1024×768, $f_{ver}=75$ Гц

Як бачимо, при переході до режиму зі збільшенням кількості пікселів та частоти кадрової розгортки, крім більш чіткої деталізації зображень (див. рис. 1 *б* по відношенню до рис. 1 *а*) відбувається і незначний зсув зображення на екрані монітору. Саме зсув зображення стає припоною до запровадження пасивних методів захисту інформації шляхом хаотичної зміни f_{ver} під час роботи монітору. Якщо не позбутися цього явища зміна частоти кадрової розгортки призводитиме до смикання зображення на екрані монітору.

Проте це є лише задачею створення відповідного програмного забезпечення, завдяки якому зображення не піддається зсувам, коли період кадрової розгортки екрану монітору хаотично змінюється в певному діапазоні періодів від $T_{\text{к min}}$ до $T_{\text{к max}}$. Необхідно, щоб це відбувалося таким чином, аби n -й час накопичення інформації $T_{ап}$ для фіксованого значення $T_{кп}$ складав не більше одиниць секунд, а при можливості – був і меншим.

Розрахунок рівня захищеності інформації можна подати коефіцієнтом:

$$\eta = \exp\left[\frac{2}{T_{\text{к max}}+T_{\text{к min}}}\int_{T_{\text{к min}}}^{T_{\text{к max}}} w(T_{\text{к}})dT\right] = \exp\left[\frac{2T_{\text{к max}}-2T_{\text{к min}}}{T_{\text{к max}}+T_{\text{к min}}}\right].$$

1. Markus G. Kuhn: Compromising emanations: eavesdropping risks of computer displays. Technical Report UCAM-CL-TR-577, University of Cambridge, Computer Laboratory, December 2003. 167 p.