ПЕРЕХОПЛЕННЯ СИГНАЛУ ВИТОКУ ІНФОРМАЦІЇ З ЕКРАНУ МОНІТОРА

Наконечний Т. А., аспірант; Євграфов Д. В., к.т.н, доцент
КПІ ім. Ігоря Сікорського, м. Київ, Україна

За допомогою побічних електронних випромінювань і наведень (ПЕВМІН) електронної техніки можливе перехоплення інформації, що циркулює в технічних пристроях, та її відновлення. На початку 80-х це суттєво вплинуло на побудову військової апаратури в США та інших провідних країнах світу.

Перехоплення та реконструкцію зображення монітора з електро-променевою трубкою (ЕПТ) персонального комп'ютера вперше продемонстрував Ван Ек у 1985. Для реконструкції зображення він використав, телевізійний приймач, синхронізовані генератори імпульсів, керовані вручну осцилятори. Схему пристрою показано на рис. 1 [1,2].

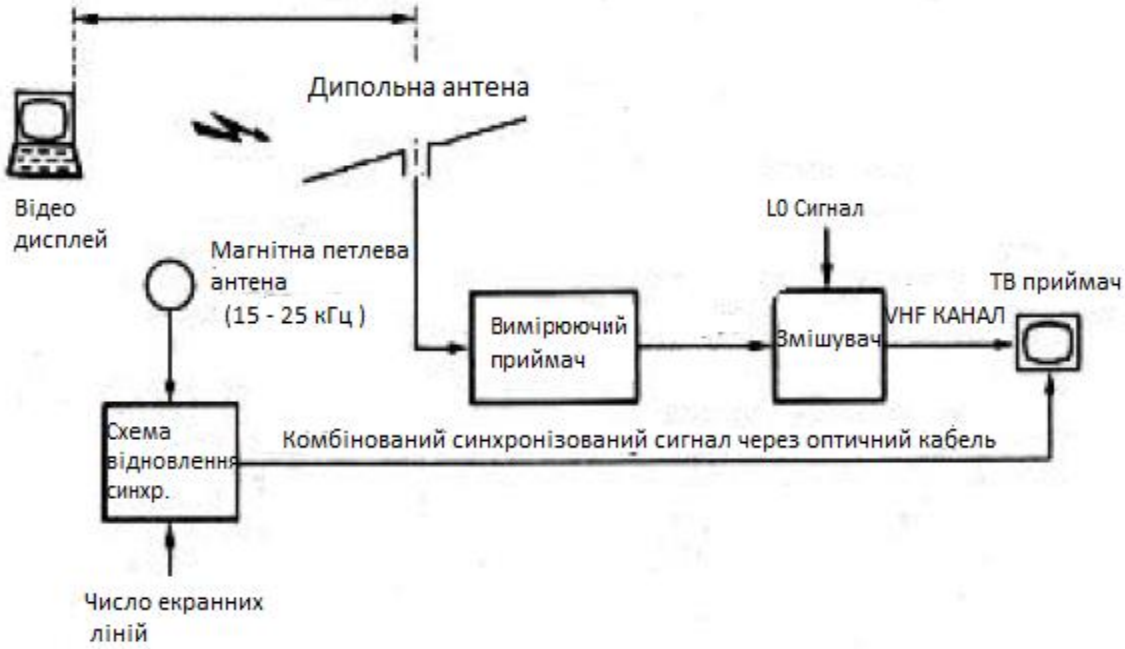

Рис. 1. Схема пристрою перехоплення.

Випромінений сигнал ділиться на:

– вузькосмуговий сигнал, а саме сигнал, який в роботі [1] має назву «clock».

широкосмуговий сигнал відео імпульсів.

Кожна гармоніка широкосмугового сигналу складає спектр телевізійного сигналу.

Перехоплення сигналу можливе з декількох сотень метрів, якщо використовується спрямована антена та підсилювач. На відміну від телевізійного сигналу, перехоплений сигнал немає частот синхронізації, тому потрібно відновлювати синхронізацію.

Найпростіший і дешевий спосіб реконструкції на екрані синхронізації

в телевізійному приймачеві є використання пристрою, який містить два осцилятори:

– регульований генератор з робочими частотами 15–20 кГц для генерації сигналу горизонтальної синхронізації (синхронізація рядків).

– регульований генератор з робочими частотами 40–80 Гц для генерування сигналу вертикальної синхронізації (синхронізація зображень).

Обидва сигнали можуть бути об'єднані і подані в розділювач синхронізації телевізійного приймача. Налаштувати обидва осцилятори на відео-дисплеї або терміналі синхронізації частоти дуже складно, тому що вони обидва повинні постійно коригуватись під час прийому [1].

Відомо, що вертикальна і горизонтальна частоти синхронізації пов'язані виразом:

$$f_{hor} = k \cdot f_{ver},$$

де f_{hor} — горизонтальна частота синхронізації, f_{ver} – вертикальна частота синхронізації, k — кількість рядків відображення на ЕПТ або екрані.

Тому практично можливо відтворювати лише горизонтальну частоту синхронізації, і отримати вертикальну частоту методом ділення:

$$f_{ver} = \frac{f_{hor}}{k}.$$

Як тільки кількість ліній екрану визначено, синхронізація може бути відновлена шляхом регулювання частоти лише одного осцилятора. На рис. 1 показано налаштування прослуховування, в якому використовується цей тип відновлення синхронізації.

Технологія перехоплення і відтворення для LCD дисплеїв подібна до технології дисплеїв з ЕПТ. Оскільки на відміну від ЕПТ в LCD дисплеях потрібно зберігати відеолінії в цифровій пам'яті, вони вимагають інформацію не лише, як бінарні закодовані кольори пікселів, але і як послідовність дискретних значень пікселів.

Сучасна LCD панель повинна оновлювати вміст від 65 до 85 раз за секунду так само, як і в електронно-променевій трубці. Це безперервне оновлення гарантує, що сигнали на відео інтерфейсі є періодичними між змінами відображеної інформації, а спектр їх складається з вузьких ліній, що відрізняються від частоти повторення [2].

Для перехоплення сигналу був використаний супергетеродинний приймач Dynamic Sciences R1250. Вихід приймача амплітудно-модульованого АМ сигналу був налаштований на відображення в режимі реального часу на звичайному моніторі комп'ютера, чиї лінії синхронізації керувались програмуючим генератором довільної форми сигналу та відтворювали рядок і частоту кадрів цільового дисплея [2].

Для прикладу розглянуто перехоплення сигналу з монітору ноутбука Toshiba Satellite Pro 440CDX, який працював у Linux середовищі у відеорежимі 800×600 пікселів і f_{ver} = 75 Гц. Антена була розташована на відстані 3

м у тій же кімнаті, що й цільовий пристрій. Швидка перевірка різних частот в діапазоні 50–1000 МГц показала, що установка в АМ приймачі центральної частоти 350 МГц і проміжної частоти смуги пропускання 50 МГц дали один з найяскравіших сигналів. Показане зображення є середнім з 16 записаних кадрів. Читабельний текст чітко виділяється з фонового шуму. Рамки були записані з частотою дискретизації 250 МГц [2].

Сигнал, перехоплений з LCD дисплею, відрізняється від типового з ЕПТ такими характеристиками:

– низькочастотні компоненти відеосигналу не ослаблені, а горизонтальні яскраві рядки з'являються у реконструйованому не просто як пара імпульсів перемикання в кінцевих точках, як це буде у випадку ЕПТ.

– шрифти втрачають половину своєї горизонтальної роздільної здатності, але є все ще такими, що можуть бути прочитаними.

– у режимі відео спостереження 800×600 пікселів і f_{ver}=75 Гц можна отримати чіткий сигнал на центральній частоті, близькій до 350 МГц, із смугою пропускання 50 МГц, але слабкіші сигнали також присутні на вищих і нижчих частотах, зокрема після кожного кроку в 25 МГц.

Перелік посилань

1. W. Van Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?", Computers & Security, No.4, August 1985.

2. Markus G. Kuhn, "Compromising emanations: eavesdropping risks of computer displays", Technical Report, University of Cambridge, Computer Laboratory, December 2003.

Анотація

Представлений огляд розробок пристроїв перехоплення інформації з дисплеїв ПК, а саме електронно-променевої трубки та LCD екранів. Наведено схему, яка відображає принцип відтворення зображення. Показано різницю відтвореного зображення між ЕПТ та LCD.

Ключові слова: монітор, ЕПТ, LCD.

Аннотация

Представлен обзор разработок устройств перехвата информации с дисплеев ПК, а именно электронно-лучевой трубки и LCD экранов. Приведена схема, отображающая принцип отображения. Показано различие воспроизводимого изображения между ЭЛТ и LCD.

Ключевые слова: монитор, ЭЛТ, LCD

Abstract

A review of developments of devices for intercepting information from PC displays, namely, a cathode-ray tube and LCD screens. The diagram, that shows the principle of image reproduction, has been presented. The difference between the reproduced image from CRT and LCD has been demonstrated.

Keywords: monitor, CRT, LCD.