УДК 621.391.63

А. А. Шпилевой, А. А. Персичкин

О ВОЗМОЖНОСТИ АНАЛИТИЧЕСКОГО ОБНАРУЖЕНИЯ СИГНАЛА ПЭМИН В ВИДЕОИНТЕРФЕЙСАХ СТАНДАРТА HDMI

Балтийский федеральный университет им. И. Канта, Калининград, Россия
Поступила в редакцию 18.07.2022 г.
Принята к публикации 03.08.2022 г.

Для цитирования: *Шпилевой А. А., Персичкин А. А.,* О возможности аналитического обнаружения сигнала ПЭМИН в видеоинтерфейсах стандарта HDMI // Вестник Балтийского федерального университета им. И. Канта. Сер. Физико-математические и технические науки. 2022. №1. С. 34—39.

Представлены теория и практическое доказательство возможности обнаружения сигнала ПЭМИН в цифровых видеоинтерфейсах. Проведен сравнительный анализ возможности снятия информации с видеоинтерфейсов VGA и HDMI посредством ПЭМИН. В соответствии с результатами анализа выдвинуто теоретическое предположение, далее доказанное на практике.

Ключевые слова: видеоинтерфейс, ПЭМИН, информационная безопасность, канал утечки, HDMI, цифровой видеоинтерфейс

Самая высокая информативность в плане устройств обработки информации, пожалуй, характерна для демонстрационных устройств, таких как мониторы, экраны, телевизоры и т. п. ПЭМИН с данных устройств образуются ввиду формирования сигнала в видеоподсистеме, включающей в себя монитор, соединительный кабель, видеоадаптер, видеоинтерфейс. Важная часть всей этой видеоподсистемы — видеоинтерфейс передачи информации.

Уходящий в историю аналоговый видеоинтерфейс VGA оставил ощутимый след в исследованиях образования и перехвата ПЭМИН интерфейсов. Множество устройств и по сей день включают в себя возможность аналогового VGA-соединения. Таким образом, плавными шагами исследования аналоговых интерфейсов перетекают в симбиоз аналогового-цифровых исследований.

На данный момент, без сомнения, самым популярным видеоинтерфейсом можно назвать High Definition Multimedia Interface (HDMI) — мультимедийный интерфейс высокой четкости. В связи с этим актуальной становится проблема обнаружения и измерения параметров сигналов ПЭМИН с указанных видеоустройств [1; 2].

Для видеоинтерфейсов, основанных на технологии VGA, подходы к обнаружению ПЭМИН базируются на понимании процесса формирования сигнала частоты смены пикселей монитора F_P [3] и определяются формулой

$$F_{\text{пэмин}} = \frac{F_p}{2} = \frac{\text{разрешение монитора} \times \text{частота кадровой развёртки}}{2} \times k\,,$$

где k — коэффициент, учитывающий технические особенности конкретной модели монитора (для современных моделей k=1,1…1,3) [4]. Таким образом, для монитора VGA с разрешением 1920×1080 и кадровой разверткой 60 Гц, диапазон поиска сигнала ПЭМИН будет в пределах 68,429—80,870 МГц. Обнаружение конкретной частоты в указанном диапазоне проводится аудиовизуальным методом путем модуляции изображения с экрана монитора [4] (рис. 1).

На рисунке 1 показан интерфейс программы SDRuno и поиск в нем интересующих нас частот. Монитор Philips 273V, интерфейс VGA, разрешение экрана 1920×1080, частота кадровой развертки 60 Гц, тестирование в режиме «строчка через строчку».

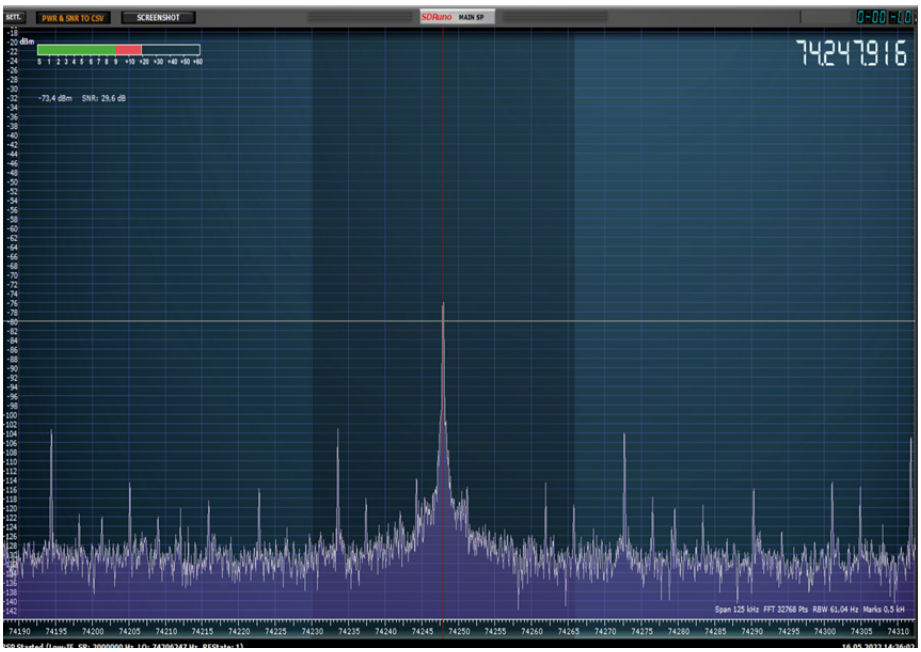

Рис. 1. Основная частота ПЭМИН (74 248 МГц) интерфейса VGA монитора Philips 273V (разрешение 1920×1080, кадровая развертка 60 Гц, SNR = 29,6 дБ)

Используемая в цифровых видеоинтерфейсах TMDS (Transition Minimized Differential Signaling) технология дает нам данные для аналитического предположения о формировании видеосигнала в интерфейсе HDMI. Сигнал в цифровых видеоинтерфейсах HDMI и DVI схож с аналоговыми видеоинтерфейсами и формируется из трех цветовых каналов. Передаваемые бинарные последовательности из 8 бит задают цветовую яркость. Таким образом, мы имеем три дифференциальные цветовые пары и одну синхропару.

Каждый пиксель изображения передается по трем цветовым каналам синхронно. Код для определенной составляющей (красный, зеленый,

синий) представляет собой последовательность из 8 битов. В TMDS происходит 8b/10b-кодирование, и из имеющихся у нас 8 битов для каждой составляющей пикселя мы получаем 10-битовый набор, который передается через проводник. Структура TMDS в источнике сигнала и приемнике симметрична, из чего следует последующее превращение 10-битового набора обратно в 8 бит. Получается, что для обнаружения ПЭМИН от HDMI алгоритм для аналогового VGA-видеоинтерфейса неприменим по следующим причинам [5]:

• частоты передачи информации (полоса поиска сигнала) в интерфейсе HDMI выше, чем в интерфейсе VGA, так как каждый уровень сигнала пикселя проходит дополнительное 8-разрядное последовательное аналого-цифровое преобразование;

• даже если будет определена рабочая полоса частот, метод модуляции экрана не позволит получить точное значение частоты сигнала ПЭМИН, так как 8-разрядный код дополняется двумя избыточными битами для повышения помехоустойчивости, что приводит к трансформации спектра.

Таким образом, можно предположить, что информационный сигнал ПЭМИН видеоинтерфейса HDMI в 10 раз выше, чем VGA, так как каждый уровень пикселя кодируется 10-битной последовательностью (8 бит АЦП, 2 бита помехоустойчивое кодирование).

Данное предположение было подтверждено экспериментально (рис. 1, 2). Рисунок 2 содержит интерфейс программы SDRuno. Для поиска частот использовались тот же монитор (Philips 273V), что и в предыдущем случае (для аналогового сигнала), та же частота кадровой развертки и тот же режим тестирования, но был изменен интерфейс с аналогового на цифровой.

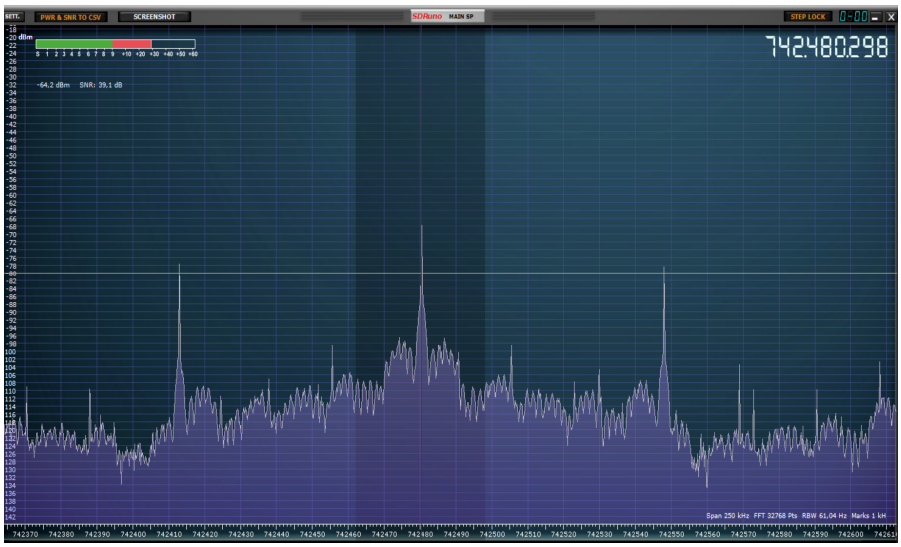

Рис. 2. Основная частота ПЭМИН (742 480 МГц) интерфейса HDMI Philips 273V (разрешение 1920 × 1080, кадровая развертка 60 Гц, SNR = 39,1 дБ)

Анализируя полученные практические результаты, можно сказать, что интересующий нас сигнал находится на частоте, в 10 раз большей, чем в аналоговом варианте. Так как параметры и монитор оставались прежними, а менялся только видеоинтерфейс передачи данных, можно предложить следующий вариант нахождения частоты ПЭМИН в цифровом интерфейсе: необходимо определить подобное значение для аналогового интерфейса и десятикратно увеличить.

Получается, что благодаря технологии TMDS, используемой в цифровых интерфейсах DVI и HDMI, значение частоты ПЭМИН благодаря кодированию 8b/10b и последующей передаче сигнала при помощи усилителя частоты десятикратно превосходит эквивалентное значение аналогового сигнала.

Таким образом, мы получаем аппроксимированную формулу для поиска частот ПЭМИН цифровых интерфейсов:

$$F_{пэмин} = \frac{разрешение\ монитора \times частота\ кадровой\ развертки}{2} \times k \times 10.$$

Помимо этого спецификация HDMI предполагает передачу на монитор сигнала с тактовой частотой $F_p \times 10$ (также является опасным) для работы цифро-аналогового преобразователя. Сигнал с указанной частотой также был обнаружен экспериментально. На рисунке 3 представлена экспериментальная проверка тактовой частоты $F_p \times 10$. Монитор (Philips 273V), та же частота кадровой развертки 60 Гц и режим тестирования «строчка через строчку», цифровой видеоинтерфейс HDMI.

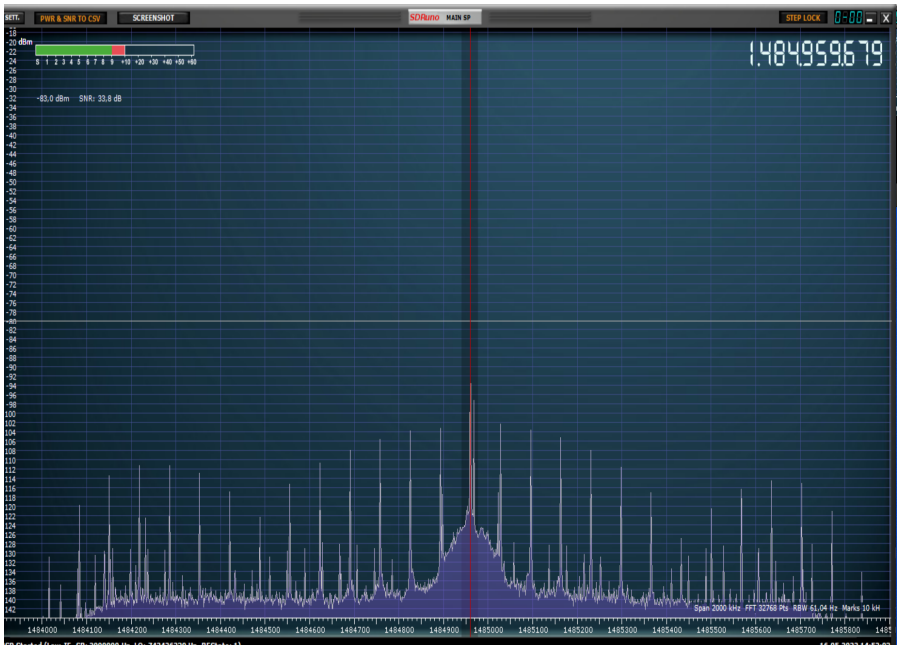

Рис. 3. Частота ПЭМИН (1 484 960 МГц) интерфейса HDMI Philips 273V (разрешение 1920×1080, кадровая развертка 60 Гц, SNR = 33,8 дБ), образованная сигналом $F_p \times 10$

Таким образом, полученные результаты позволяют предположить следующую методику обнаружения сигналов ПЭМИН в мониторах, работающих в режиме HDMI:

1. Стандартной методикой определяется основная частота сигнала ПЭМИН — $F_{пэмин}$ указанного монитора в режиме VGA.

2. Искомые основные частоты ПЭМИН монитора в режиме HDMI будут равны $F_{пэмин} \times 10$ и $F_{пэмин} \times 20$.

Примечание: исследуемый монитор должен иметь два видеоинтерфейса: VGA и HDMI.

В результате мы получили новую методику нахождения частот полезных сигналов в цифровых видеоинтерфейсах. Данная методика основана на аналитическом предположении о различии в процессе формирования аналогового и цифрового видеосигнала. Принципиальным же является наличие в HDMI-интерфейсе технологии TMDS. Дифференциальная передача сигналов с минимизацией перепадов уровней и осуществляемое 8b/10b-кодирование десятикратно увеличивают частоту, на которой находится информативный сигнал. Произведенное практическое исследование (поиск частот) при помощи RTL-SDR (resistor-transistor logic software defined radio) приемника (программно определяемая радиосистема на основе резисторно-транзисторной логики) позволяет нам убедиться в точности определения частот по новой методике и целесообразности использования методики в случае поиска цифровых частот для известных аналоговых значений частот. Данная работа была выполнена для упрощения взаимодействия с цифровыми интерфейсами и упрощения «оцифровки» мира.

Список литературы

1. *Сборник* временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. М., 2002.

2. *Специальные* требования и рекомендации по технической защите конфиденциальной информации (СТР-К) : утв. приказом Председателя Гостехкомиссии России от 30 августа 2002 г. №282. М., 2001.

3. *Гук М.* Аппаратные интерфейсы ПК. Энциклопедия. СПб., 2002.

4. *Программа* формирования тестов на ПЭМИН «Сигурд-Тест» : руководство пользователя МСШЕ.503300.005РП / ООО «Центр безопасности информации «МАСКОМ».

5. *Интерфейс* HDMI // Блог программиста : [сайт]. URL: https://pro-prof.com/forums/topic/интерфейс-hdmi (дата обращения: 15.07.2022).

Об авторах

Андрей Алексеевич Шпилевой — канд. физ.-мат. наук, доц., Балтийский федеральный университет им. И. Канта, Калининград, Россия.

E-mail: AShpilevoi@kantiana.ru

Андрей Андреевич Персичкин — ст. преп., Балтийский федеральный университет им. И. Канта, Калининград, Россия.

E-mail: a.persichkin@kgnic.ru

A.A. Shpilevoy, A.A. Persichkin

ON THE POSSIBILITY OF ANALYTICAL DETECTION OF THE TEMPEST SIGNAL IN HDMI VIDEO INTERFACES

Immanuel Kant Baltic Federal University, Kaliningrad, Russia
Received 18 July 2022
Accepted 03 August 2022

To cite this article: Shpilevoy A.A., Persichkin A.A. 2022, On the possibility of analytical detection of the TEMPEST signal in HDMI video interfaces, *Vestnik of Immanuel Kant Baltic Federal University. Series: Physical-mathematical and technical sciences*, №1. P. 34–39.

This paper presents the theory and the practical proof of the possibility of detecting the TEMPEST signal in digital video interfaces. A comparative analysis of the possibility of obtaining information from VGA and HDMI video interfaces by means of TEMPEST was carried out. In accordance with the results of the analysis, a theoretical assumption was put forward and practically proved later.

Keywords: video interface, TEMPEST, Information Security, leak channel, HDMI, digital video interface

The authors

Dr Andrey A. Shpilevoy, Associate Professor, Immanuel Kant Baltic Federal University, Kaliningrad, Russia.
E-mail: AShpilevoi@kantiana.ru

Andrey A. Persichkin, Assistant Professor, Immanuel Kant Baltic Federal University, Kaliningrad, Russia.
E-mail: a.persichkin@kgnic.ru