

A.A. Golyakov, E.V. Dirienko

Analysis of Compromising Emanations from a Laser Printer Printing Head for the Purpose of Assess the Possibility of Information Interception

Keywords: compromising emanations, analysis of compromising emanations from a laser printer printing head, laboratory testing compromising informative signal.

This article shows how to calculate and extract the desired harmonic of compromising informative signal from a laser printer printing head. There are the formulas for determining the frequency of the testing compromising informative signal for extracting of it in the particular frequency range. Also it shows in detail the process of radio scanning and authenticating compromising informative signal from a laser printer printing head.

A.A. Голяков, Е.В. Дириенко

**ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПОЛУЧЕНИЯ ИНФОРМАЦИИ
С ПЕЧАТАЮЩЕГО БЛОКА ЛАЗЕРНОГО ПРИНТЕРА ПО КАНАЛУ ПЭМИ**

В настоящее время достаточно подробно проработаны вопросы проведения специсследований утечки информации с видеомониторов за счет побочных электромагнитных излучений и наводок (ПЭМИН). Стоит учесть, что информация может быть перехвачена не только с видеомониторов, но также и с различных периферийных устройств (принтер, сканер, плоттер, копировальный аппарат, выносные устройства хранения информации и т.д.), которые используются для хранения, изготовления и размножения документов, а значит, могут хранить, и обрабатывают информацию, содержащую конфиденциальные сведения. К сожалению, в настоящее время этот вопрос недостаточно хорошо проработан. Например, в статье М.С. Чистякова и А.П. Дураковского «Основы проведения специальных исследований средств изготовления и размножения документов» говорится только о выборе критериев классификации средств изготовления и размножения документов, что является лишь основой для проведения специсследований [1]; в статье О.Н. Маслова, М.А. Соломатина, В.Д. Егоренкова «Тестовые сигналы для анализа ПЭМИН периферийных устройств персональных ЭВМ» рассмотрены характеристики тестовых сигналов, используемых для исследования ПЭМИН мониторов и периферийных устройств (сканеров и принтеров) персональных ЭВМ (ПЭВМ), показаны информативные сигналы и их параметры от различных интерфейсов периферийных устройств [2]. Однако в данных статьях ничего не говорится об исследовании печатающего блока лазерного принтера на предмет выявления тестового сигнала по каналу ПЭМИН. Не так много полезной информации можно найти о проведении специсследований принтеров, в частности печатающих блоков лазерных принтеров, в открытых и закрытых источниках.

В данной работе рассмотрен печатающий блок лазерного принтера HP LaserJet 1100.

Проанализируем технические характеристики данного принтера:

- технология печати – лазерная;
- максимальный формат – А4;
- максимальное разрешение для ч/б печати – 600×600 dpi;
- скорость печати – 8 стр/мин (ч/б А4);
- интерфейс – LPT.

Попробуем на основании имеющихся данных рассчитать тактовую частоту работы лазерного диода при тесте «пиксель через пиксель». Для этого напечатаем в данном режиме лист формата А4 и измерим линейкой размер печатной области, получаем – 8,03×11,38 дюймов.

Расчёт количества точек на листе формата А4 (с учётом полей):

$$N_{\text{кол-во точек на листе А4(с учётом полей)}} = 8,03 \times 11,38 \times 600 \times 600 = 32\,897\,304.$$

По техническим характеристикам принтера скорость печати:

$$8 \text{ стр/мин} \approx 0,13 \text{ стр/с или } 1 \text{ страница за } 7,5 \text{ с.}$$

Данный показатель учитывает также время захвата и выброса листа, которое не следует учитывать при определении тактовой частоты тестового сигнала на лазерном диоде. Предполагаем, что на захват и выброс листа принтер затрачивает 2 с. Таким образом, для печати одной строки принтеру необходимо следующее время:

$$\frac{5,5}{11,38 \times 600} = 8,055 \times 10^{-4} \text{ с.}$$

Очевидно, что не все это время будет использоваться непосредственно для печати, принтеру необходимо какое-то время на сдвиг листа бумаги для печати следующей строки. Следовательно, в расчетную формулу необходимо ввести коэффициент, который будет учитывать время, затраченное непосредственно на печать строки – назовём его коэффициентом использования $K_{\text{и}}$.

$$K_{\text{и}} = \frac{\text{Время, затраченное принтером на одну строку}}{\text{Время, затраченное на сдвиг листа}}.$$

Физически данный коэффициент показывает, во сколько раз возрастет частота печати пикселей при меньшем времени, затраченном непосредственно на печать, относительно времени, затраченного на одну строку.

Предполагаем, что время на сдвиг листа равно половине времени печати строки. Таким образом, непосредственно на печать строки будет затрачено 0,4 мс, а $K_{\text{и}} = 2$.

Данное предположение подтверждает осциллограмма, снятая с лазерного диода при времени развертки 0,1 мс, рис. 1. Из осциллограммы видно, что период следования широких импульсов (при которых и происходит непосредственно печать строки) занимает около 0,8 мс, длительность импульса печати занимает около 0,36 мс.

К сожалению, характеристики осциллографа не позволили непосредственно получить осциллограммы информативных импульсов.

Таким образом, конечная формула для расчета тактовой частоты лазерного диода приобретает следующий вид:

$$F_{\text{лаз.диода на практ.}} = \frac{N_{\text{кол-во точек на листе А4(с учётом полей)} * K_{\text{и}}}{5,5 * 2} = 5,981 \approx 6 \text{ МГц.}$$

К сожалению, при использовании имеющегося оборудования (программно-аппаратный комплекс «Сигурд-М2», в составе которого: анализатор спектра R&S ESPI3 и измерительная дипольная антенна АИ5-0 с УР-1.6) не удалось наблюдать сигнал от печатающего блока принтера в штатном режиме его работы.

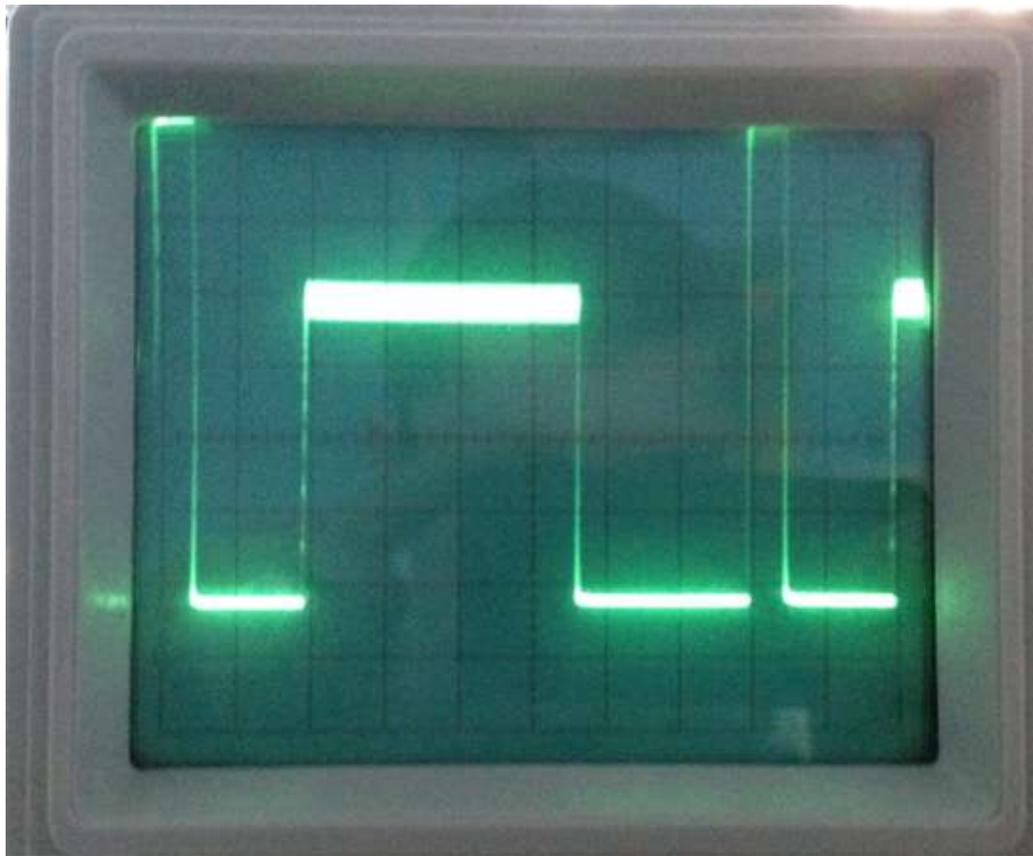


Рис. 1. Осциллограмма, снятая с лазерного диода

Для получения более мощного излучения гармоники тестового сигнала внесём асимметрию в цепь информативного сигнала печатающего блока лазерного принтера (рис. 2), разорвав канал передачи информации непосредственно на лазерный диод и соединив его петлёй, образованной медным проводом длиной примерно 50 см (рис. 3).

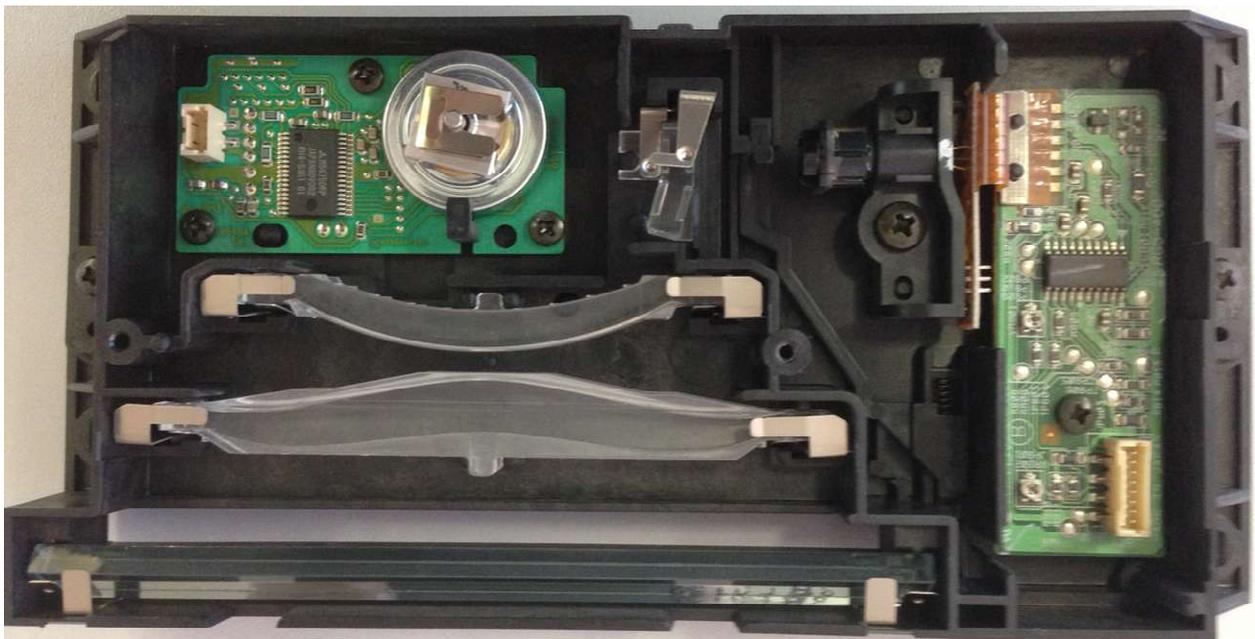


Рис. 2. Печатающий блок лазерного принтера HP LaserJet 1100

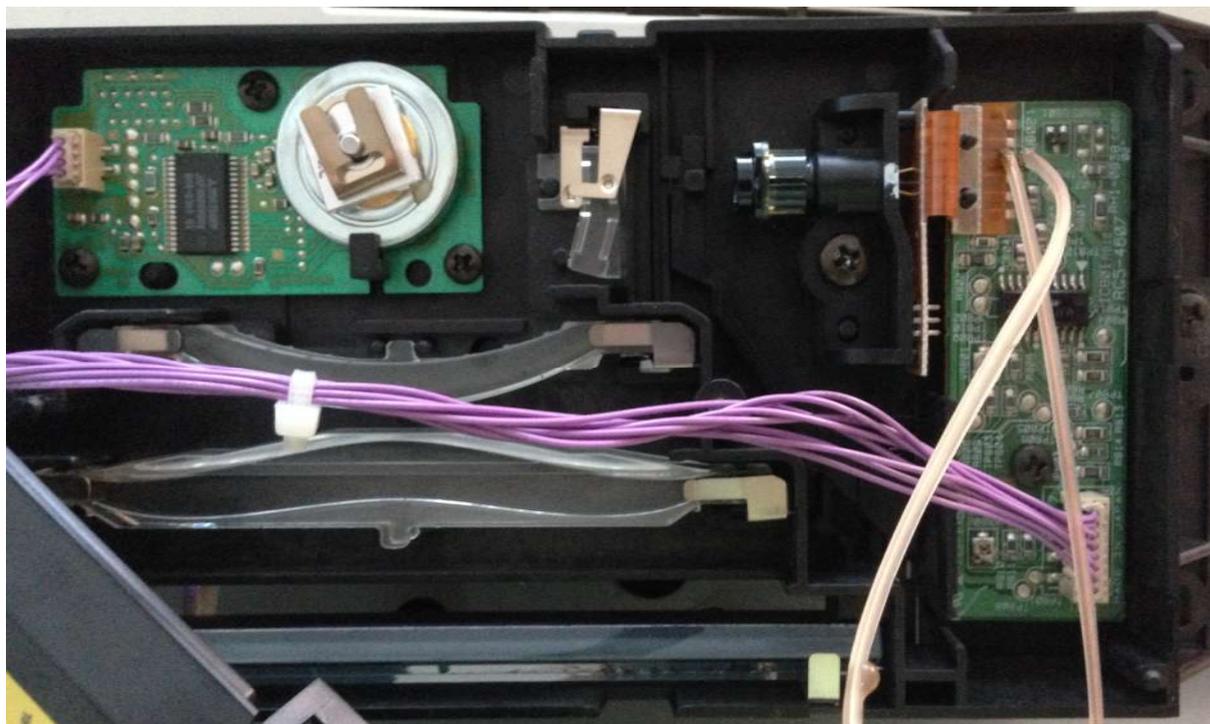


Рис. 3. Модифицированный печатающий блок лазерного принтера HP LaserJet 1100

Как было рассчитано, первая гармоника тестового сигнала, при печати листа пиксель через пиксель, должна находиться примерно на частоте 6 МГц. С учетом погрешностей наших предположений первая гармоника тестового сигнала найдена на частоте 6,153 МГц, рис. 4.

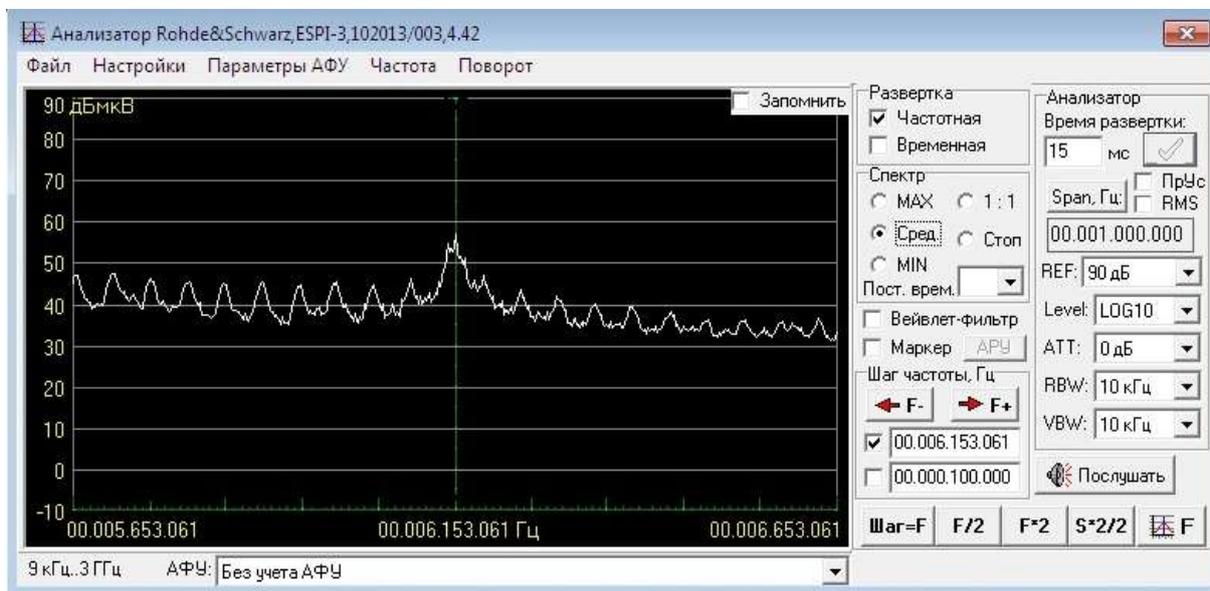
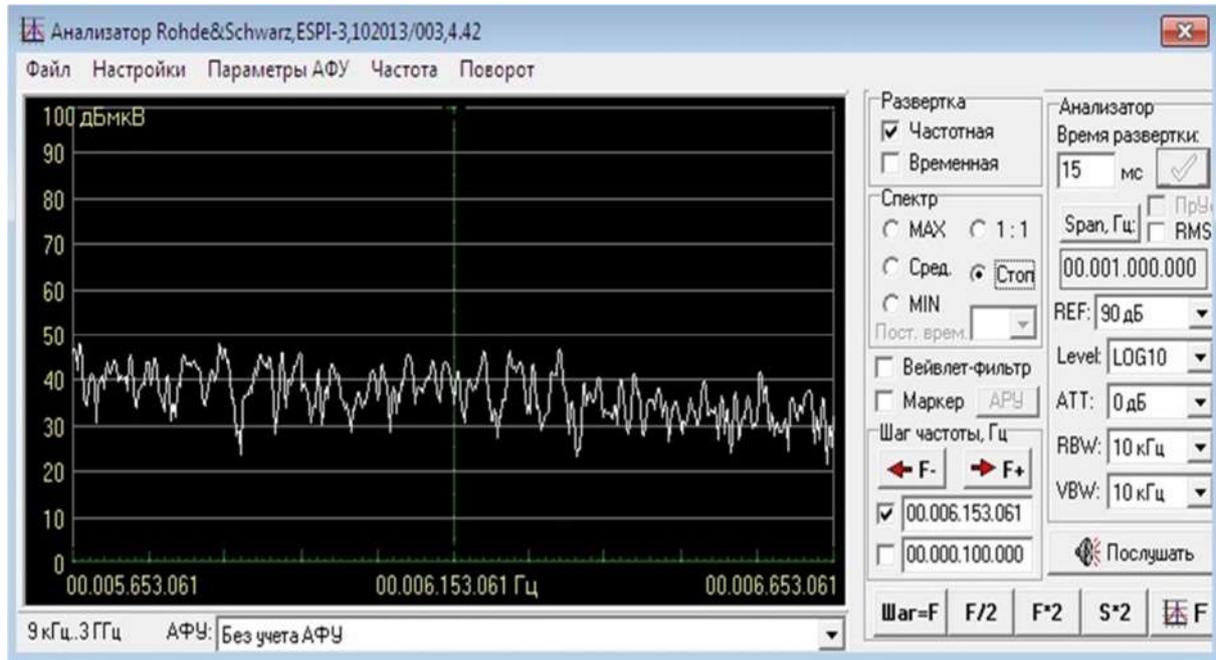


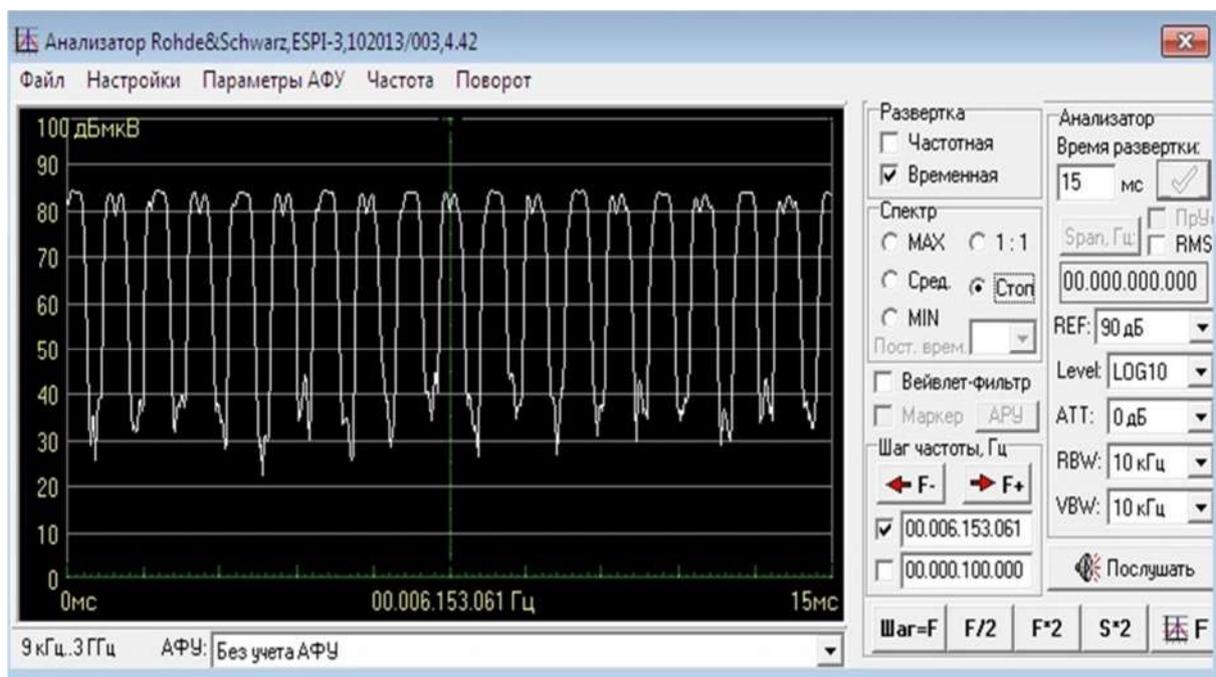
Рис. 4. Окно анализатора спектра R&S ESPI3 на частоте 6,153 МГц при печати страницы пиксель через пиксель на лазерном принтере

При печати пустого листа на принтере данной гармоника не видно (рис. 5), что доказывает, что найденная гармоника тестового сигнала является опасным (информативным) сигналом, поступающим на лазерный диод принтера.

Также идентифицируем данный сигнал во временной области при печати страницы пиксель через пиксель и пустой страницы (рис. 6, 7). Как видно на рис. 6 и 7, разница заметна невооруженным взглядом.



*Рис. 5. Окно анализатора спектра R&S ESPI3 на частоте 6,153 МГц при печати
пустой страницы на лазерном принтере*



*Рис. 6. Окно анализатора спектра R&S ESPI3 во временной области на частоте
6,153 МГц при печати страницы пиксель через пиксель на лазерном принтере*

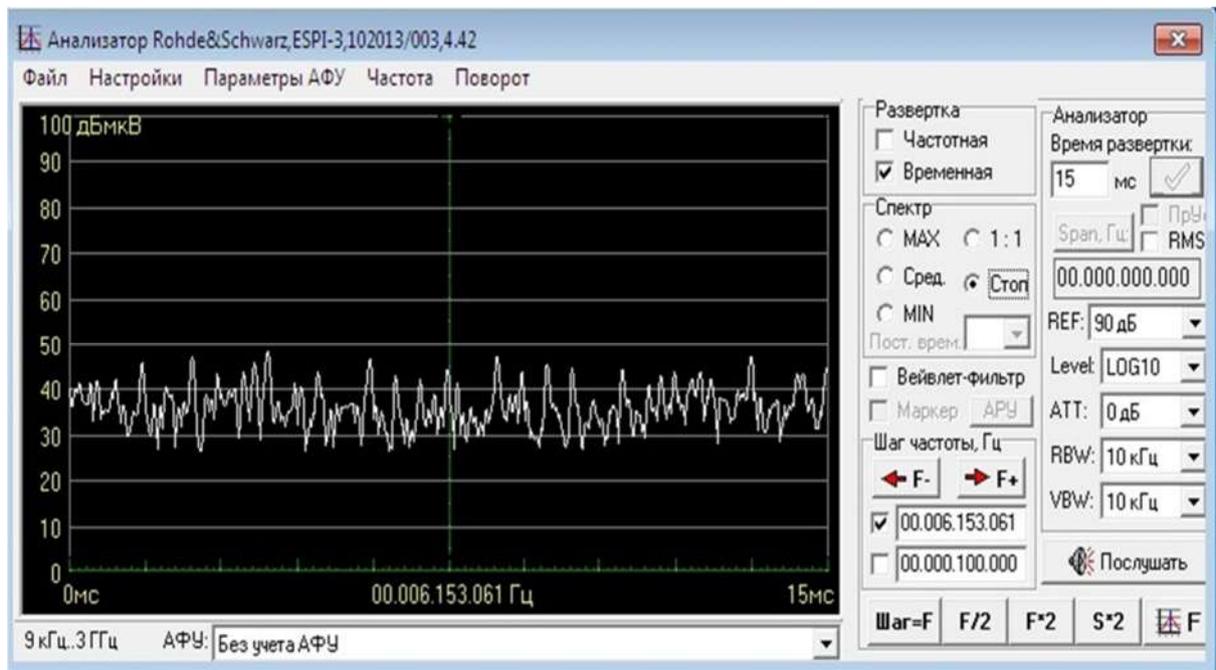


Рис. 7. Окно анализатора спектра R&S ESPI3 во временной области на частоте 6,153 МГц при печати пустой страницы на лазерном принтере

Убедимся также, что это именно 1 гармоника, а не 2 или 3, напечатав страницу пиксель через 2 пикселя. При такой печати страницы в теории 1 гармоника должна появиться на частоте вдвое меньшей, чем при печати страницы пиксель через пиксель, а именно на частоте 3,076 МГц (рис. 8). Посмотрим также на данную частоту при печати во временной области (рис. 9).

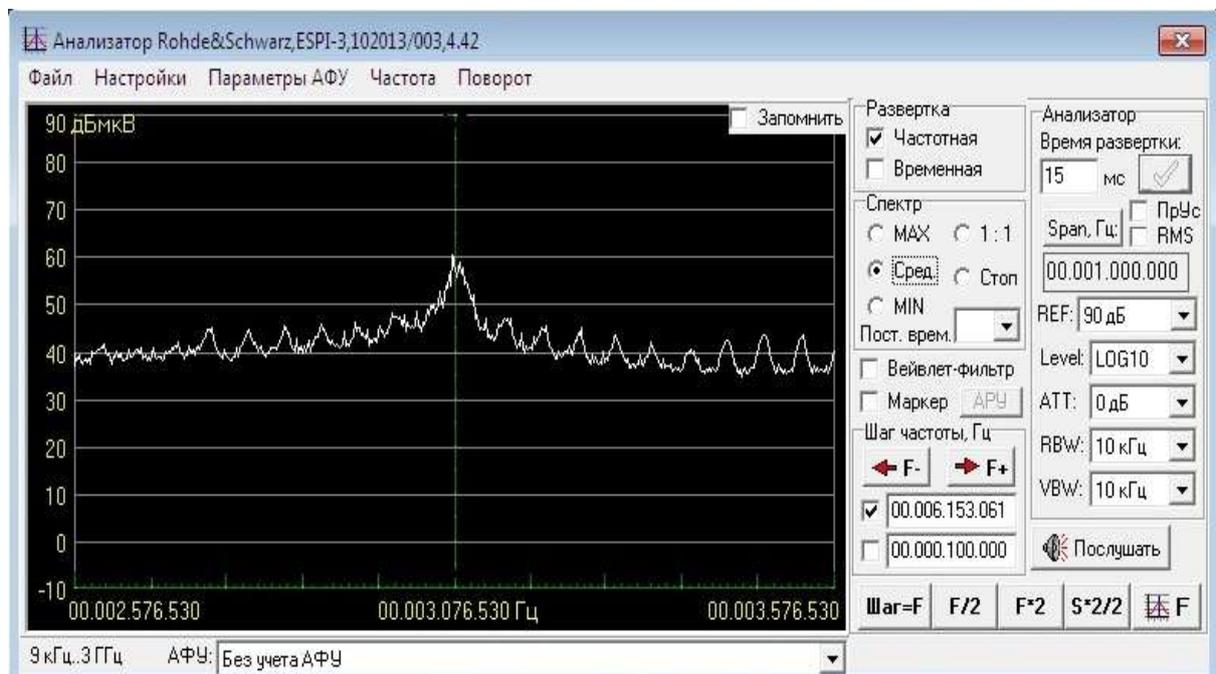


Рис. 8. Окно анализатора спектра R&S ESPI3 на частоте 3,076 МГц при печати страницы пиксель через 2 пикселя на лазерном принтере

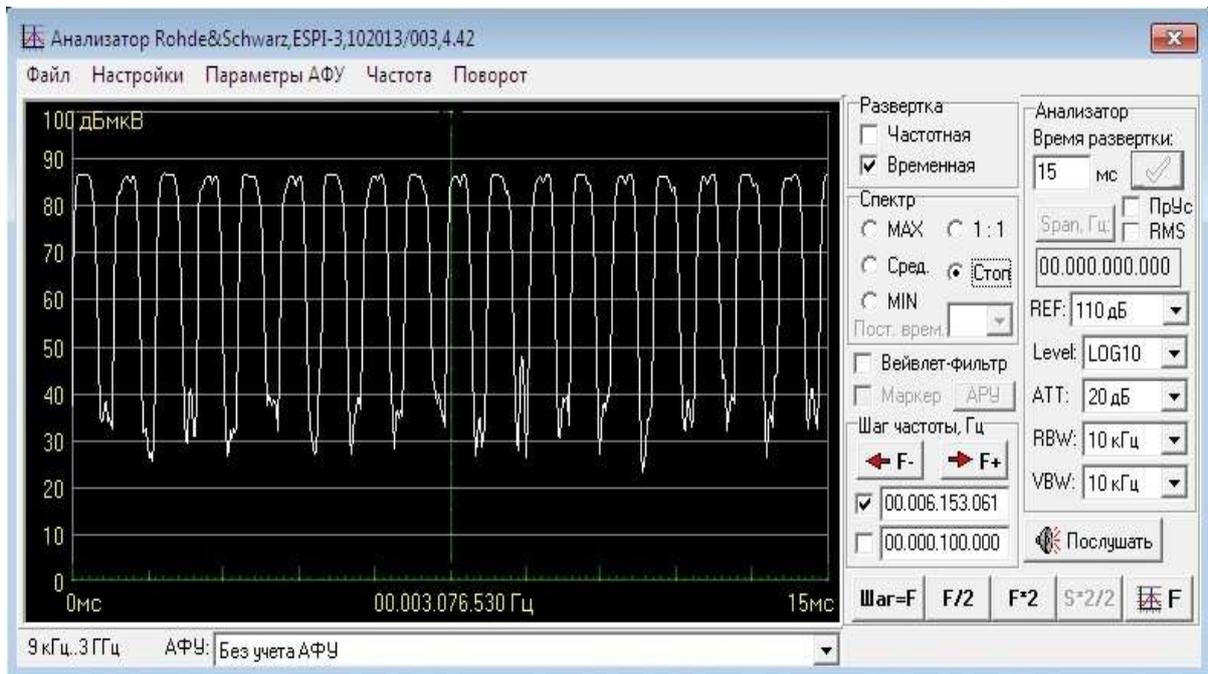


Рис. 9. Окно анализатора спектра R&S ESPI3 во временной области на частоте 3,076 МГц при печати страницы пиксель через 2 пикселя на лазерном принтере

Напечатаем также страницу пиксель через 7 пикселей, чтобы окончательно убедиться, что это именно наш тестовый сигнал, и что 1 гармоника находится именно на частоте 6,153 МГц. При такой печати страницы первая гармоника должна появиться на частоте в 7 раз меньше 6,153 МГц, т.е. на частоте 879 кГц (рис. 10). Рассмотрим также во временной области частоту 879 кГц при печати страницы пиксель через 7 пикселей (рис. 11).

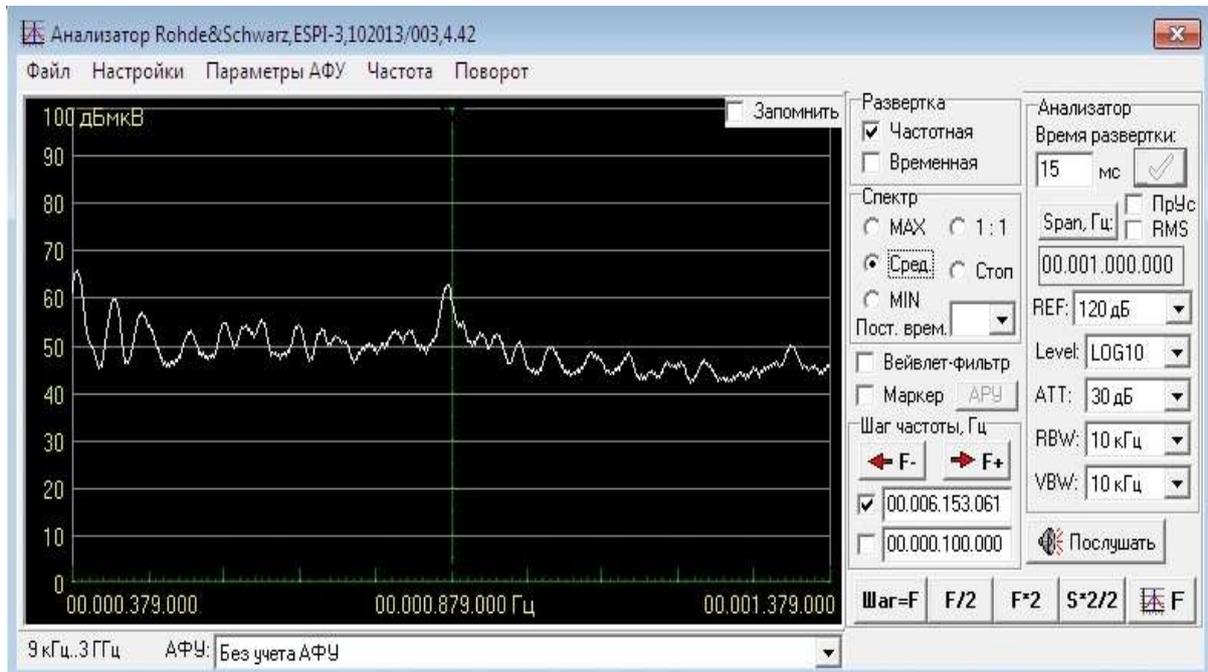


Рис. 10. Окно анализатора спектра R&S ESPI3 на частоте 879 кГц при печати страницы пиксель через 7 пикселей на лазерном принтере

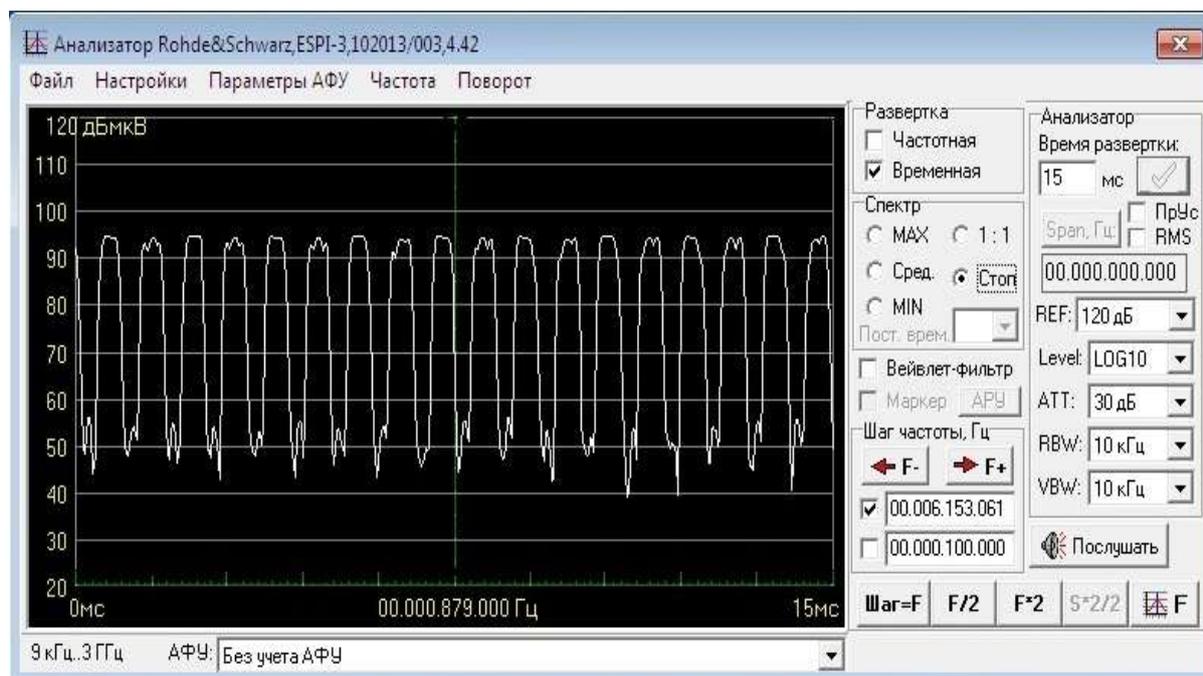


Рис. 11. Окно анализатора спектра R&S ESPI3 во временной области на частоте 879 кГц при печати страницы пиксель через 7 пикселей на лазерном принтере

Так как никаких других гармоник между тактовыми частотами тестовых сигналов обнаружено не было, частота 6,153 МГц является 1-й гармоникой тестового сигнала в режиме печати пиксель через пиксель.

Данное исследование показывает, что снятие информации возможно с печатающего блока лазерного принтера. Что в свою очередь доказывает важность проведения специсследований для организаций, занимающихся технической защитой информации в процессе аттестации объектов информатизации.

СПИСОК ЛИТЕРАТУРЫ:

1. Чистяков М.С., Дураковский А.П. Основы проведения специальных исследований средств изготовления и размножения документов // Безопасность информационных технологий. 2011. №1. С.130.
2. Маслов О.Н., Соломатин М.А., Егоренков В.Д. Тестовые сигналы для анализа ПЭМИН периферийных устройств персональных ЭВМ // Инфокоммуникационные технологии. 2007. Т.5, № 2. С.82-83.

REFERENCES:

- Chistyakov M.S., Durakovskiy A.P. Osnovy provedeniya spetsialnykh issledovaniy sredstv izgotovleniya i razmnozheniya dokumentov // Bezopasnost informatsionnykh tekhnologiy №1. P. 130.
- Maslov O.N., Solomatin M.A., Egorenkov V.D. Testovye signaly dlya analiza PEMIN periferiynykh ustroystv personalnykh EVM // Infokommunikatsionnye tehnologii. 2007. V.5, № 2. P. 82-83.