ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 537.811

О НЕКОТОРЫХ ПРОБЛЕМАХ ПРИ ОЦЕНКЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО КАНАЛУ ПЭМИ

Васильев Андрей Савельевич,
старший преподаватель кафедры безопасности и информационных технологий

Рыжиков Сергей Сергеевич,
доцент кафедры безопасности и информационных технологий

Агуреев Иван Александрович,
заведующий учебной лабораторией кафедры безопасности и информационных технологий Национальный исследовательский университет "МЭИ", 111250, Россия, г. Москва, Красноказарменная улица, дом 14, e-mail: universe@mpei.ac.ru

Аннотация

В процессе проведения специальных исследований по оценке уровня побочных электромагнитных излучений (ПЭМИ) от средств вычислительной техники (СВТ) приходится сталкиваться с определенными проблемами, которые не находят должного уровня в нормативно-методических документах Федеральной службы по техническому и экспертному контролю (ФСТЭК) России. В данной статье предпринята попытка рассмотреть некоторые из них.

Ключевые слова: ПЭМИ, ФСТЭК России, зона R2, специальные исследования

ABOUT SOME PROBLEMS IN ASSESSING THE SECURITY OF INFORMATION FROM LEAKAGE THROUGH THE PMI CHANNEL

Andrey S. Vasilyev,
Senior Lecturer at chair of Security and Information Technology

Sergey S. Ryzhikov,
postdoctoral reseacher at chair of Security and Information Technology

Ivan A. Agureev,
head of educational laboratory, chair of Security and Information Technology
National Research University "Moscow Power Engineering Institute", Krasnokazarmennaya st.,14, Moscow, Russia, 111250, email: universe@mpei.ac.ru

ABSTRACT

In the process of conducting special studies to assess the level of spurious electromagnetic radiation (PEMI) from computer technology (CBT), one has to face certain problems that do not find the proper level in the regulatory and methodological documents of the Federal Service for Technical and Expert Control (FSTEC) of Russia. This article attempts to cover some of them.

Keywords: PMI, FSTEC of Russia, Zone R2, special studies

Введение

Современная техника обработки информации характеризуется низким уровнем сигналов побочных электромагнитных излучений. Низкий уровень ПЭМИ является следствием ужесточения санитарных норм и требований электромагнитной совместимости, что в свою очередь предъявляет повышенные требования к точности измерений.

Для проведения специальных исследований и контроля защищенности конфиденциальной информации, обрабатываемой на ПЭВМ, по каналу ПЭМИ необходимо последовательно провести следующие операции:

выполнить обнаружение сигналов ПЭМИ;

произвести измерение пикового значения амплитуды сигнала ПЭМИ и среднеквадратического значения уровня шума;

провести расчет требуемых показателей защищенности.

Для поиска ПЭМИ от современных средств вычислительной техники используются специальные алгоритмические, методические и организационные подходы [1].

Методические требования к проведению измерений

Организационные мероприятия в процессе проведения лабораторных (стендовых) специальных исследований заключаются в создании наилучших условий для излучения, распространения и приема сигналов ПЭМИ.

С этой целью:

на измерительном столе размещается весь проверяемый комплект СВТ;

приемная антенна располагается в непосредственной близости от излучающих узлов и блоков исследуемой техники;

производится распрямление кабелей, по которым передается информация для придания им лучших антенных свойств;

обеспечение персоналом корректности действий при проведении измерений.

Необходимо стремиться к тому, чтобы исключить дополнительные возмущения электромагнитного поля при проведении специальных исследований:

тестируемая аппаратура и тестирующая аппаратура должны находиться друг от друга на максимальном удалении;

нельзя допускать передвижение людей и предметов в помещении во время проведения исследований;

оператор должен находиться всегда в одном и том же месте (после проведения ручных операций он должен возвращаться на свое место);

на время исследований не включать в помещении, где проводятся исследования, никаких устройств, создающих дополнительные помехи.

В процессе проведения лабораторных (стендовых) специальных исследований после обнаружения информативных ПЭМИ от исследуемого устройства, уточнения номиналов частот основного излучения и его гармоник, необходимо корректно измерить их уровень,

т.е. пиковые значения амплитуд излучений при включенном тестовом сигнале и уровень индустриального шума при выключенном тесте.

Для этого необходимо соблюсти ряд условий:

настроиться на максимальный лепесток диаграммы направленности ПЭМИ за счет вращения измерительного стола с исследуемым комплектом СВТ;

выбрать правильный вектор поляризации антенны;

разместить антенну на расстоянии 1 метр от исследуемого устройства;

использовать рекомендуемую методикой измерения полосу пропускания, соответствующую занимаемой полосе частот ПЭМИ.

Пиковые значения сигналов произвольной формы измеряются пиковым детектором, так как он обладает малым временем заряда и большим время разряда. Это позволяет фиксировать максимальные всплески сигнала за время измерения, которое следует устанавливать не менее 1/10 используемой полосы пропускания. Результат измерения данным детектором отвечает смыслу термина «амплитуда сигнала».

Для измерения индустриального шума (спектральной плотности мощности шума) следует применять детектор среднеквадратических значений. Результат измерений данным детектором имеет смысл среднеквадратичной мощности шума.

Несоблюдение этих условий значительно исказит (как правило, в сторону уменьшения) пиковые значения амплитуд побочных излучений, что скажется на точности вычислений.

Сканирование частотного диапазона до 30 МГц на предмет поиска ПЭМИ от СВТ следует проводить в соответствие с требованиями методики ФСТЭК России с полосой пропускания 9 (10) кГц; в пределах 30 – 100 МГц – с полосой 30 кГц, а свыше 100 МГц – с полосой 100 (120) кГц.

Данные рекомендации хорошо работают при достаточно узких сигналах таких как ПЭМИ, образуемые интерфейсом VGA. Несмотря на широкое развитие современных цифровых интерфейсов, он имеет широкое распространение и еще долгое время будет эксплуатироваться.

Сложнее дело обстоит с цифровыми видео интерфейсами, например, DVI, в основе которого лежит технология TMDS.

Измерение широкополосных побочных излучений

Интерфейс DVI является синхронным, т.е. передача данных осуществляется строго по тактам, в соответствии с тактовыми сигналами, формируемыми на отдельной линии. Передача данных осуществляется по дифференциальным парам, что обеспечивает высокую помехозащищенность интерфейса, позволяя добиться высокой пропускной способности. При этом ПЭМИ наблюдаются на более высоких частотах по сравнению с VGA.

Тактовая частота первой гармоники DVI интерфейса при стандартных разрешениях не выше 1600 × 1280 × 60 Гц лежит в пределах 130…170 МГц. В этом случае полосы пропускания 100 (120) кГц оказывается недостаточно для сбора всей энергии ПЭМИ.

В настоящее время в устройствах отображения СВТ широко применяются жидкокристаллические дисплеи с активной матрицей (TFT LCD) — разновидность жидкокристаллического дисплея, в котором используется активная матрица, управляемая тонкоплёночными транзисторами.

Необходимость соблюдения жёстких международных норм по уровню ПЭМИ с точки зрения электромагнитной совместимости определяет применение производителями TFT матриц как методов передачи цифровых данных дифференциальными сигналами с малыми перепадами уровня напряжения (200-400 мВ) – интерфейсы RSDS (Reduced Swing

Differential Signaling) и LVDS (Low Voltage Differential Signaling), так и угловой модуляции тактовой частоты в этих интерфейсах.

Спектр электромагнитного излучения матрицы монитора вместо острых пиков становится размытым, приобретая форму, представленную на спектрограмме (рис. 1,2).

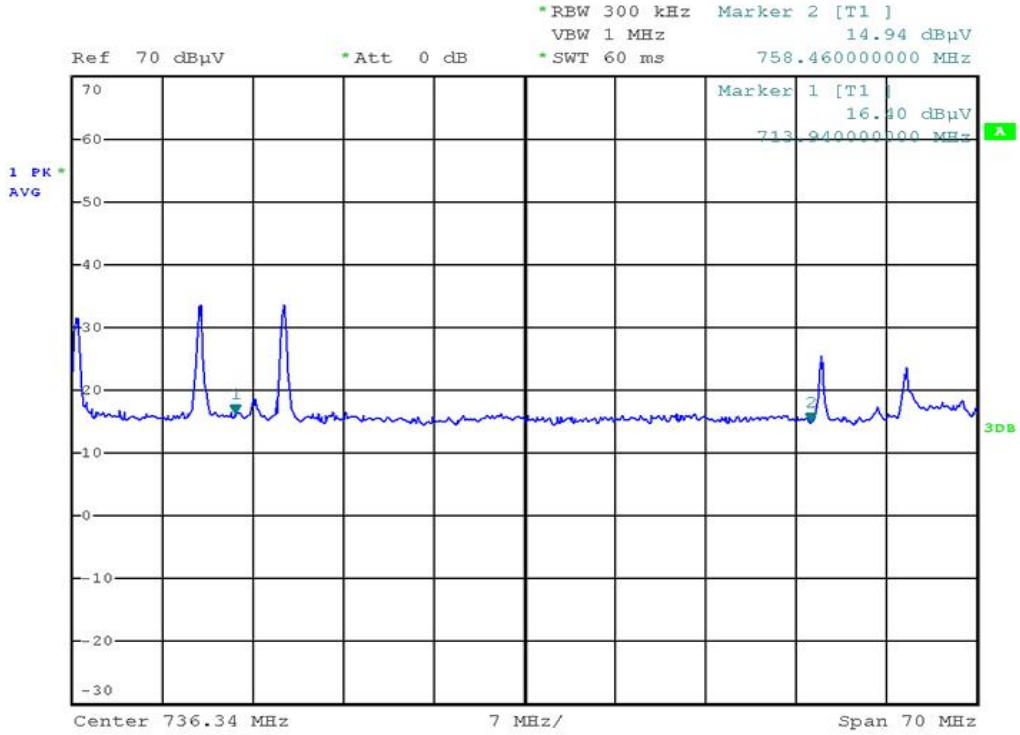

Рисунок 1. Излучение TFT матрицы монитора (тест выкл.)

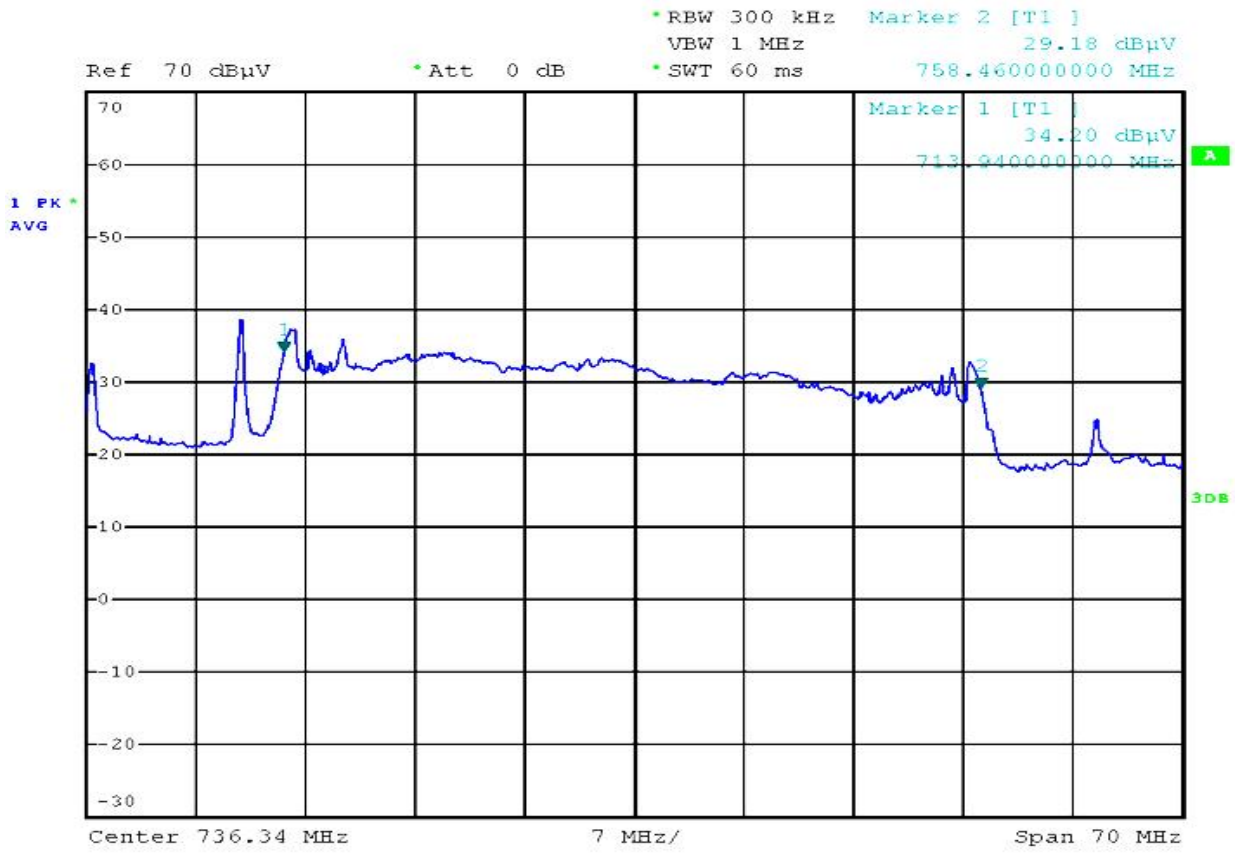

Рисунок 2. Излучение TFT матрицы монитора (тест вкл.)

TFT матрица не единственный источник широкополосных сигналов, которые проявляются в ходе проведения специальных лабораторных исследований. Аналогичные

побочные излучения с расширенным спектром можно наблюдать и от картридера SD – карт, присутствующего во многих моделях ноутбуков.

На рисунках 3 и 4 соответственно представлены ПЭМИ картридера на основной частоте (1-я гармоника) и ПЭМИ, соответствующее 7-й гармонике сигнала. Уровни фоновых излучений при отключенном тестовом сигнале отображены синим цветом, побочные излучения от считывателя SD – карт при включенном тестовом сигнале – желтым.

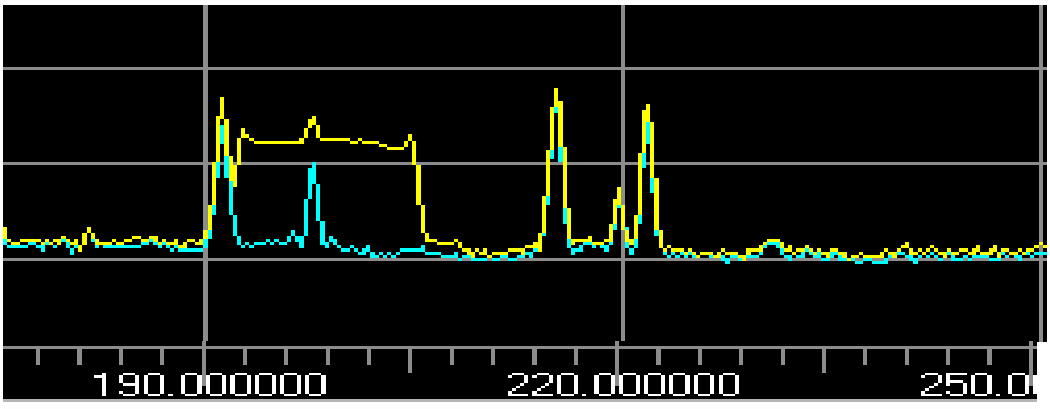

Рисунок 3. ПЭМИ основной частоты SDX

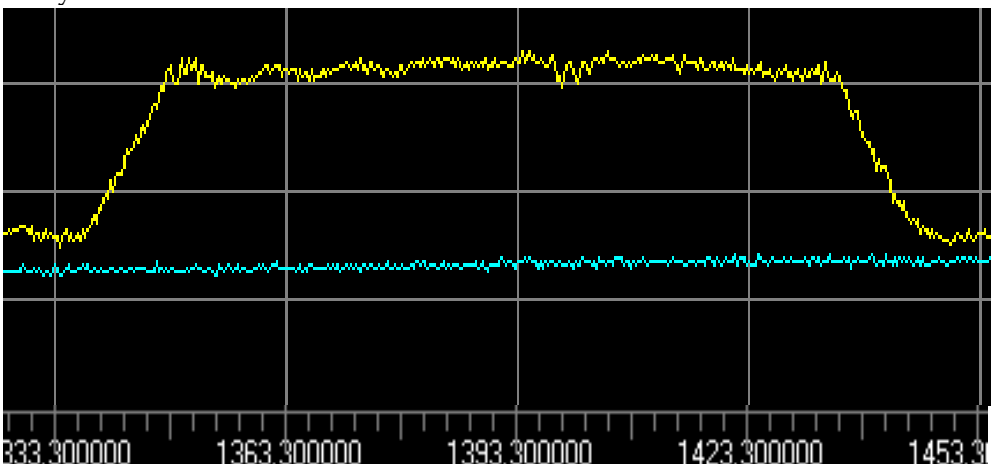

Рисунок 4. 7-я гармоника ПЭМИ SDX

Подобное размытие спектра излучения значительно затрудняет его обнаружение с рекомендованной методикой ФСТЭК России полосой пропускания приемника 100 кГц-120 кГц. Поэтому поиск подобных ПЭМИ целесообразно проводить при значениях полосы пропускания приемника 300 кГц. После обнаружения всех гармоник побочных излучений и уточнения точных номиналов частот необходимо провести измерение уровней всех ПЭМИ с целью расчета такого ключевого показателя защищенности информации как зона R2 - пространства вокруг технического средства обработки информации, в пределах которого отношение "опасный сигнал/помеха" для составляющих напряженности электромагнитного поля превышает допустимое нормированное значение.

И здесь возникает дилемма – проводить измерения, установив в анализаторе спектра полосу пропускания равную или несколько больше, чем ширина спектра ПЭМИ, или, в соответствии с нормативными документами, измерять, нарезая спектр побочного излучения на фрагменты по 100 (120) кГц, с последующим их пересчетом для реальной ширины спектра излучения.

При первом подходе измерения более корректны с точки зрения радиотехники, но при этом не позволяют учитывать энергию отдельных более узкополосных помех, которые могут присутствовать спектре измеряемого ПЭМИ (рис. 3).

Второй подход соответствует требованиям нормативных документов и позволяет исключить энергию помех (при их наличии) из расчета уровня ПЭМИ, но при пересчете фрагментов спектра применительно к реальной полосе частот, занимаемой побочным излучением, легко потерять часть энергии ПЭМИ. Данная потеря неизбежно скажется на точности расчета показателей защищенности.

Факторы, влияющие на точность измерений

Рассмотрим факторы, влияющие в конечном итоге на точность результатов оценки R2.

Погрешности коэффициентов калибровки электрических измерительных антенн и допускаемой погрешности измерений.

Согласно [2] погрешность определения коэффициентов калибровки электрических измерительных антенн в диапазоне частот до 1 ГГц не должна превышать + 2,0 дБ, а в диапазоне частот свыше 1ГГц не должна превышать + 1,5 дБ.

Пределы допускаемой погрешности измерений напряженности электрического поля составляют + 3,0 дБ [3].

Установка уровня контрастности монитора

В процессе оценки ПЭМИ от матрицы TFT монитора с целью расчета зоны R2 уровень побочного излучения может значительно меняться в зависимости от режима «яркость-контрастность» тестового изображения, выводимого на монитор (рис. 5). При этом в методических документах ФСТЭК России данное явление никак не регламентировано.

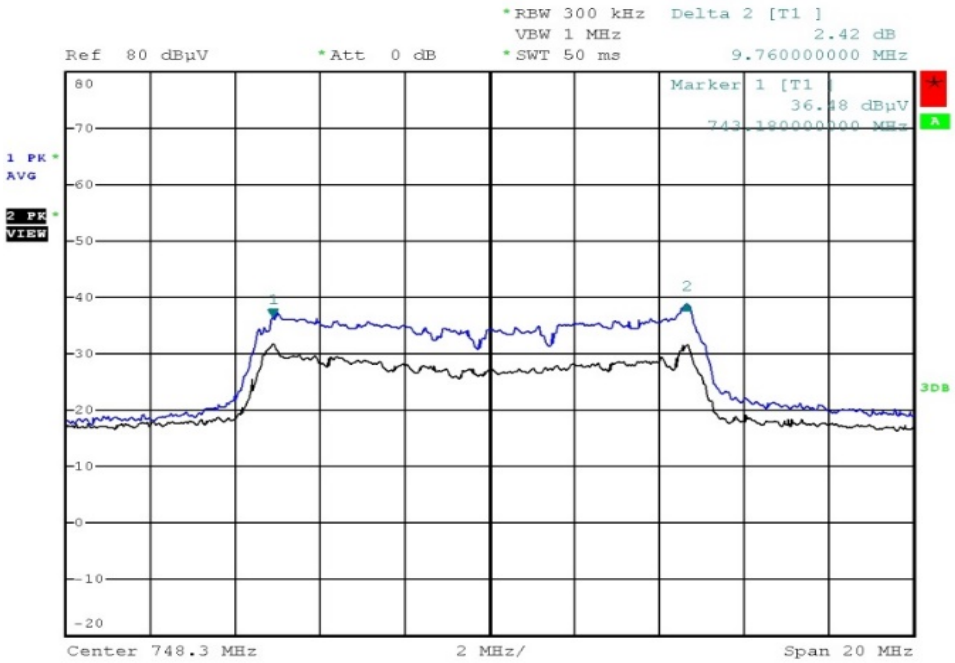

Рисунок 5. Изменение уровня ПЭМИ TFT матрицы монитора в зависимости от режима «яркость-контрастность» тестового изображения

Таким образом, получить в процессе измерений ошибку в несколько дБ вполне реально. При этом «недобор» в 3-4 дБ при расчете величины зоны R2, например, для DVI интерфейса и разрешения экрана монитора 1280x1024 пикселей с частотой обновления 60 Гц, может вызвать ошибку в сторону уменьшения в зависимости от частоты ПЭМИ более десятка метров.

Следовательно, расчетная величина зоны R2 получится меньше реальной.

Заключение

В завершении статьи хотелось бы остановиться на существующих программах для генерации тестовых режимов в исследуемых средствах вычислительной техники и периферийном оборудовании при проведении специальных исследований.

В настоящее время на рынке предлагаются различные наборы тестовых программ для управления работой подсистем ПЭВМ и периферийного оборудования с целью формирования сигналов ПЭМИ заданного вида, например: НАВИГАТОР-ТЕСТ1 (ЗАО НПЦ Фирма «НЕЛК»), СИГУРД-ТЕСТ (Группа компаний МАСКОМ), Сборник тестовых программ для ОС Windows (ООО «Центр безопасности информации»).

При этом тестовая программа задает в исследуемом устройстве некий режим генерации периодических сигналов в электрических цепях, которые в свою очередь вызывают появление информативных побочных излучений в радиоэфире.

Основное требование к тестовой программе – обязательное наличие в тестовом сигнале постоянной комбинации, что определяет неизменные характеристики ПЭМИ по амплитуде и частоте.

Проблема состоит в том, что подобное не всегда возможно как по причине преобразования в процессе передачи самого информационного потока (кодирование, шифрование), так и за счет применения скремблирования с целью рандомизации спектральных компонентов передаваемых модулированных сигналов.

Например, в ЛВС 100Base-T4 – применяется алгоритм кодирования данных 8B/6T, метод физического кодирования NRZI и аппаратного скремблирования - наложения псевдослучайной последовательности на информационный битовый поток.

В интерфейсе DisplayPort к передаваемым данным применяется 128-битное AES-кодирование [4].

В интерфейсе USB версии 3.0 и выше используется скремблирование путем поразрядного суммирования по mod2 информационной последовательности символов с М-последовательностью, образованной полиномом X16 + X5 + X4 + X3+ 1 [5]. При этом реальный сигнал в линии приобретает свойства ПСП.

Таким образом, преобразование информационного потока данных и/или его скремблирование не позволяет при существующих подходах и отсутствии соответствующих тестовых программ оценить величину зоны R2.

Подобная ситуация также никак не отражена в нормативно-методических документах ФСТЭК России.

Список литературы:

1. Программно-аппаратный комплекс поиска побочных электромагнитных излучений и наводок "Навигатор". Описание применения. ЛИБЮ.424400.012 РЭ
2. Комплексы программно-аппаратные поиска и измерения побочных электромагнитных излучений и наводок «Навигатор-ПхМ». Методика поверки. Утверждена 05.09.2016 ФГБУ «ГНМЦ» Минобороны России.
3. Описание типа средств измерений в редакции, утвержденной приказом Росстандарта № 851 от 25.04.2017г. Приложение к свидетельству № 65140 об утверждении типа средств измерений.
4. Ежов, В. Интерфейсы HDMI и DisplayPort: вопросы проектирования тестирования [Электронный ресурс]. / В. Ежов. – Режим доступа: http://www.russianelectronics.ru/
5. https://www.usb3.com/whitepapers/USB%203%200%20(11132008)-final.pdf. Universal Serial Bus 3.0 Specification - USB3.com

References:

1. "Navigator" hardware and software complex for searching for side electromagnetic emissions and pickups. Description of the application. LIBYu.424400.012 RE
2. Complexes software and hardware search and measurement of side electromagnetic radiation and pickups "Navigator-PkhM". Verification method. Approved on 09/05/2016 by the State Scientific and Research Center of the Ministry of Defense of the Russian Federation.
3. Description of the type of measuring instruments in the edition approved by order of Rosstandart No. 851 of 25.04.2017. Appendix to certificate No. 65140 on the type approval of measuring instruments.
4. http: //www.russianelectronics.ru/ HDMI and DisplayPort: Test Design Issues. Journal "Electronic Components" No. 9-2009.
5. https://www.usb3.com/whitepapers/USB%203%200%20(11132008)-final.pdf. Universal Serial Bus 3.0 Specification - USB3.com