

ЛИТЕРАТУРА

1. FTTH Council Europe Webinar – April 23rd, 2020 [Электронный ресурс]. – Режим доступа : <https://www.telepolis.pl/images/2020/04/swiatlowod-eu-092019.pdf>. – Дата доступа: 29.08.2021.
2. Юмашева, Е. С. Методы защиты волоконно-оптических линий связи / Е. С. Юмашева, В. Н. Ежгуров // Материалы конференций ГНИИ "Нацразвитие". Февраль 2018: Сборник избранных статей Международных научных конференций, Санкт-Петербург, 23–28 февраля 2018 года. – СПб. : Частное научно-образовательное учреждение дополнительного профессионального образования Гуманитарный национальный исследовательский институт «НАЦРАЗВИТИЕ», 2018. – С. 15-18.
3. Кольцов, А. С. Исследование методов защиты информации, передаваемой по волоконно-оптическим линиям связи / А. С. Кольцов, Н. В. Филатова, А. В. Пальчиков // Актуальные проблемы деятельности подразделений УИС: Сборник материалов Всероссийской научно-практической конференции, Воронеж, 25 октября 2018 года / Ответственный за выпуск Д.Г. Зыбин. – Воронеж: Издательско-полиграфический центр «Научная книга», 2018. – С. 43-46.
4. Верхозин, А. Н. Магнитооптика вчера и сегодня / А. Н. Верхозин // Вестник Псковского государственного университета. – Псков, 2015. – С. 114–124.
5. Образование, наука и технологии: проблемы и перспективы: сборник научных трудов по материалам международной научно-практической конференции, 31 октября 2019 г. / Под общ. ред. А.В. Туголукова – М. : ИП Туголуков А.В., 2019. – С. 211-215.
6. Дейнека, И. Г. Изучение магнитооптического эффекта Фарадея / И. Г. Дейнека, О.А. Шрамко, С.А. Тараканов // Научно-технический вестник информационных технологий, механики и оптики. – СПб., 2008. – С. 84–89.
7. Яворский, Б. М., Детлаф, А. А. Анализ поляризованного света. Эллиптическая и круговая поляризация света // Справочник по физике. – 4-е изд. – М.: Наука, 1968. – 940 с.
8. Верде постоянная // Физическая энциклопедия: [в 5 т.] / Гл. ред. А. М. Прохоров. — М.: Советская энциклопедия, 1988. – Т. 1: Ааронова – 707 с.

Е.Р.АДАМОВСКИЙ¹, В.К.ЖЕЛЕЗНЯК¹, С.В.ХАРЧЕНКО¹, К.Я.РАХАНОВ¹

**ИЗЛУЧЕНИЕ ЦИФРО-АНАЛОГОВОГО ПРЕОБРАЗОВАТЕЛЯ ПРИ ОБРАБОТКЕ
ТЕСТОВЫХ СИГНАЛОВ**

¹Учреждение образования «Полоцкий государственный университет», г. Новополоцк, Республика Беларусь

Введение. Повсеместное распространение цифровых устройств для решения широкого спектра задач во всех областях жизнедеятельности человека обуславливает наличие в них модулей конвертации аналоговых и цифровых сигналов друг в друга. Например, микрофоны и динамики являются устройствами ввода и вывода аналогового звукового сигнала соответственно, но при этом его хранение и обработка средством вычислительной техники (СВТ) производится в цифровом виде. Решающие задачу конвертации сигналов устройства называются аналого-цифровыми (АЦП) и цифро-аналоговыми (ЦАП) преобразователями.

В процессе работы электрическая техника формирует побочные электромагнитные излучения, которые коррелируют с обрабатываемыми в данный момент сигналами. Без надлежащих мер по защите информации в каналах утечки (КУИ) излучение может быть перехвачено и расшифровано злоумышленником с помощью специальных технических средств. Поскольку АЦП и ЦАП являются важными узлами современных СВТ, где может происходить обработка секретных данных, исследование взаимосвязи их излучений с целевыми сигналами способно дать информацию, которая может быть использована для повышения уровня защищенности подобных устройств.

В данной работе произведено исследование, в котором на внешнем модуле ЦАП происходила обработка тестовых сигналов, а излучение устройства фиксировалось магнитной антенной. Полученные результаты обработаны и подвергнуты анализу.

Схема эксперимента. В качестве ЦАП использован модуль E14-440 производства LCard [1], некоторые характеристики которого приведены в таблице 1.

Таблица 1 – Характеристики модуля E14-440

Разрядность ЦАП, бит	Частота дискретизации, кГц	Буфер ЦАП, слов	Тактовая частота процессора, МГц	Выходной ток, мА
12	62.5	512 – 4032	48	< 2

Подключение и питание осуществлялось через порт USB от изолированного управляющего персонального компьютера, использовался ноутбук HP ProBook 4540s. Аналоговый выход подключался к устройству воспроизведения звука. Использованное программное обеспечение – пакет LabView National Instruments [2] с библиотекой lview.dll производителя, чьи файлы были модифицированы для осуществления экспериментальных измерений соответствующим образом. Схема эксперимента показана на рисунке 1.

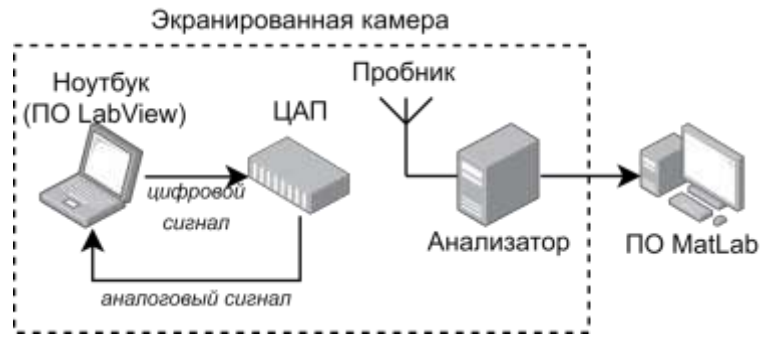


Рисунок 1 – Результаты измерений

Измерения производились в экранированной полубезэховой камере ОАО «Конструкторское бюро «Дисплей». Измерение и обработка декодированного аналогового сигнала в диапазоне 10-3000 кГц происходило при помощи анализатора Agilent N9020A [3] и индукционного токового пробника SIP9136A [4], который подключался к кабелю, соединяющему аналоговый выход ЦАП и звуковой вход ноутбука (TRS).

Результаты. В качестве эталонных состояний рассмотрены две конфигурации эксперимента: с выключенным модулем ЦАП и при обработке сигнала нулевой амплитуды. Рисунок 2 подтверждает изолированность экспериментальной установки, поскольку на графике почти отсутствуют посторонние гармоники; в режиме ожидания устройство формирует излучение с особым составом.

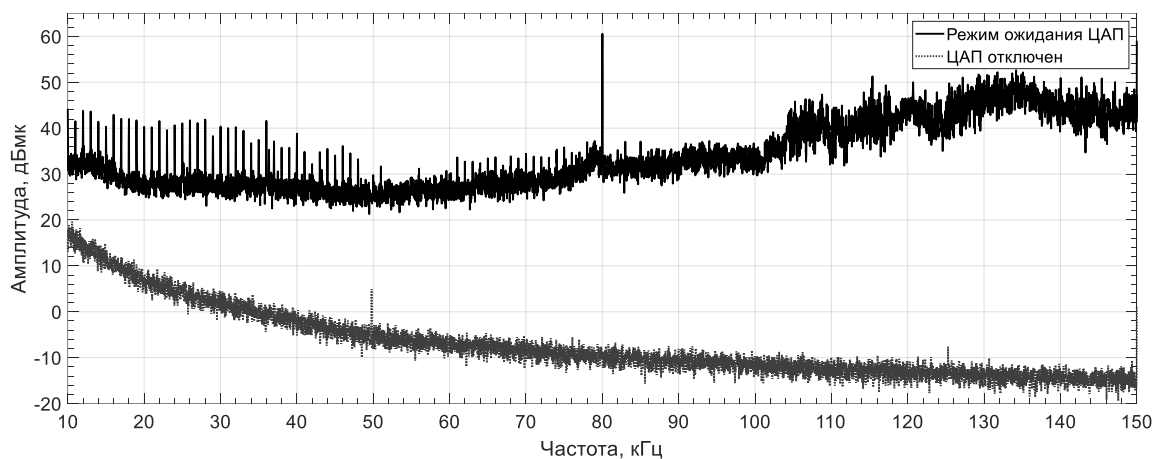


Рисунок 2 – Результаты контрольных измерений

Тестовыми сигналами послужили синусоида и периодическая треугольная последовательность с настраиваемыми параметрами частоты и амплитуды. Выбраны две частоты, одна из которых кратна частоте дискретизации ЦАП $12.5 \text{ кГц} = 62.5 \text{ кГц} / 5$, а вторая – не кратная, близкая к ней 12.38 кГц , что позволяет сравнить их на одном графике (рисунок 3).

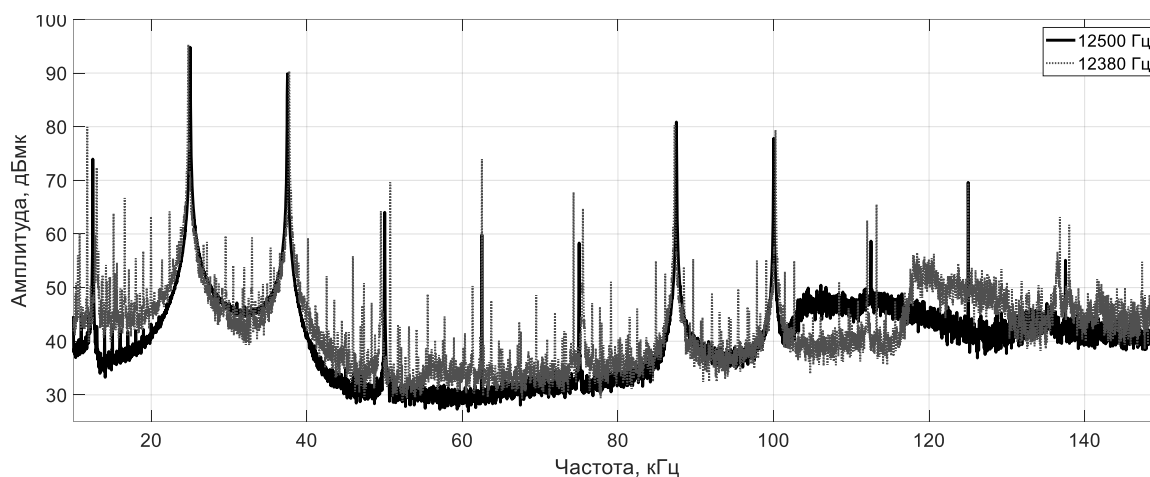


Рисунок 3 – Результаты измерений

Анализ рисунка 3 показывает, что в случае кратности частот сигнала и устройства в спектре наблюдаются высшие гармоники сигнала, включая четные и нечетные, даже при условии их отсутствия в обрабатываемом сигнале. Также присутствуют кратные гармоники самого устройства, отличающиеся более узкой формой, вызванной сосредоточением спектральных составляющих в узкой полосе.

Отсутствие кратности частот приводит к появлению множества комбинационных составляющих, о чем свидетельствует симметричное расположение гармоник относительно частоты дискретизации ЦАП. В данном случае первая гармоника исходного сигнала в спектре не наблюдается.

Заключение. Проведен практический эксперимент для получения данных об электромагнитном излучении цифро-аналогового преобразователя в процессе функционирования в зависимости от обрабатываемых им данных. Установлены особенности генерации с использованием тестовых гармонических сигналов: спектральный состав излучения обусловлен кратностью частоты сигнала и дискретизации устройства.

ЛИТЕРАТУРА

1. E14-440 Внешний модуль АЦП/ЦАП на шину USB [Электронный ресурс]. – Режим доступа : <https://www.lcard.ru/products/external/e-440>. – Дата доступа: 15.09.2021.
2. LabView National Instruments [Электронный ресурс]. – Режим доступа: <https://www.ni.com/ru-ru/shop/labview.html>. – Дата доступа: 15.09.2021.
3. Технические данные N9020A [Электронный ресурс]. – Режим доступа: <https://www.astena.ru/n9020a.html>. – Дата доступа: 27.09.2021.
4. Токовые клещи связи (10 кГц – 400 МГц) TESEQ CIP 9136 [Электронный ресурс]. – Режим доступа: <https://theseuslab.by/p53884073-tokovye-kleschi-svyazi.html>. – Дата доступа: 27.09.2021.

О.А.КОНДРАШУК¹, Е.С.БЕЛОУСОВА¹

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

¹Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Распространение беспроводных технологий привело к возникновению технологии облачных вычислений и переходу на IPv6, также в последнее время получила развитие концепция интернета вещей. Интернет вещей (Internet of Things, IoT) – концепция вычислительной сети физических предметов, оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой без вмешательства со стороны человека и передаче данных по глобальной сети с помощью протокола IP.

В современном мире интернет вещей становится неотъемлемой частью корпоративных систем во всех сферах деятельности, количество подключенных устройств стремительно растет, так же, как и объемы данных, которые они генерируют. При этом многие устройства интернета вещей до сих пор плохо защищены.