**Министерство образования и науки Республики Казахстан**

**Евразийский технологический университет**

Мольганов А.А.

**ДИПЛОМНАЯ РАБОТА**

**на тему: «Разработка аппаратно-программного комплекса для безопасной передачи сообщения по оптическому каналу связи»**

Специальность: 6B06106 – «Информатика»

Алматы 2023

**Министерство образования и науки Республики Казахстан**

**Евразийский технологический университет**

«Допущен(а) к защите»

Заведующий кафедрой

\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_

**ДИПЛОМНАЯ РАБОТА**

На тему: «Разработка аппаратно-программного комплекса для безопасной передачи сообщения по оптическому каналу связи»

Выполнил: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Мольганов А.А.

*(подпись)*

Научный руководитель: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Савельева В.В.

*(подпись)*

**Алматы 2023**

**ЕВРАЗИЙСКИЙ технологический университет**

Кафедра «Информационные технологии и сервис»

**З А Д А Н И Е**

на выполнение дипломной работы

Студенту Мольганову А.А.

Тема дипломной работы «Разработка аппаратно-программного комплекса для безопасной передачи сообщения по оптическому каналу связи»

Научный руководитель: Савельева Виктория Вячеславовна, ассоц.профессор, PhD

Утверждено приказом по университету № \_\_\_\_ от «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_\_г.

Срок сдачи законченной дипломной работы на кафедру 20.09.2020 г.

Содержание и объем работы (пояснительной, расчетной и экспериментальной частей, т.е. перечень подлежащих разработке вопросов)

1. Анализ предметной области.
2. Проектирование аппаратно-программного комплекса.
3. Оптимизация криптографического алгоритма.

Рекомендуемая основная литература

# 1. K. Mitzner, Complete PCB Design Using OrCAD Capture and PCB Editor – Second Edition. – Elseiver Academic Press, 2019. – 600 p.

# 2. Митцнер К., Доу Б., Акулин А., Супонин А., Мюллер Д., Проектирование печатных плат в OrCAD Capture и OrCAD PCB Editor, Второе издание. – Москва: Техносфера, 2022. – 592 с.

# 3. B. Griffin., Cadence Sigrity 2019 Release Function – Cadence Publisher, 2019. – 56 p.

# 4. Пош М., Программирование встроенных систем на C++ 17 / пер. с англ. А.В. Снастина. – М.: ДМК Пресс, 2020. – 394 с.

# 5. Novello K., Mastering STM32. – М.: Leanpub Publishing, 2022. – 910 p.

Перечень графического материала (с точным указанием обязательных таблиц, чертежей или графиков и т.п) Таблиц-31, Рисунков-33.

Дата выдачи задания\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Заведующий кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Полегенько И.Г. /

(подпись) (Ф.И.О.)

Руководитель дипломной работы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Савельева В.В. /

(подпись) (Ф.И.О.)

Задание принял к исполнению студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_/ /

(подпись) (Ф.И.О.)

Дата \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

СОДЕРЖАНИЕ

|  |  |  |
| --- | --- | --- |
|  | ВВЕДЕНИЕ……………………………………………………………… | 6 |
|  |  |  |
| 1 | АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ…………………………………. |  |
| 1.1 | Передача информации в открытом пространстве …………………….. | 8 |
| 1.2 | Описание целей разработки ………………………………………......... |  |
| 1.3 | Анализ существующих технологий передачи информации в открытом пространстве ………………………………………………… |  |
| 1.4 | Обоснование проектных решений……………………………………… |  |
| 2 | ПРОЕКТИРОВАНИЕ АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКСА…………………………………………………………… |  |
| 2.1 | Проектирование аппаратного обеспечения комплекса ……………..... |  |
| 2.2 | Проектирование программного обеспечения комплекса …………….. |  |
| 3 | ОПТИМИЗАЦИЯ КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА……… |  |
| 3.1 | Криптографический алгоритм AES ........................................................ |  |
| 3.2 | Аппаратные ускорители шифрования и дешифрования информации. |  |
| 3.3 | Оптимизация криптографического алгоритма AES ………………… |  |
|  | ЗАКЛЮЧЕНИЕ……………………………………………………….. |  |
|  | СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ………………….. |  |

ВВЕДЕНИЕ

В настоящее время развитие высокотехнологичных отраслей экономики любого государства невозможно без системного развития системных компетенций, которые связывают между собой отрасли и разделы науки, образования и экономики.

Информационно-коммуникационные технологии являются одним из основных факторов системного развития науки, образования и экономики любого государства. Современное развитие информационно-коммуникационных технологий требует постоянного совершенствования информационных систем и вспомогательных комплексов для эффективной передачи, обработки и хранения данных.

При проектировании критической информационной инфраструктуры, особое внимание уделяется аппаратно-программным телекоммуникационным комплексам, имеющим интерфейсы для приема и передачи информации.

Современное развитие критической информационной инфраструктуры сочетает в себе использование различных типов телекоммуникационного оборудования – коммутационные и распределительные системы, спутниковые, оптические, волоконно-оптические, беспроводные и высокоскоростные комплексы передачи данных.

Особое место в телекоммуникационном оборудовании для критической информационной инфраструктуры занимают аппаратно-программные комплексы для передачи и приема информации по атмосферной оптической линии связи.

Атмосферные оптические линии связи, а также комплексы, оборудования и системы в их составе, передают и принимают информацию при помощи электромагнитных волн оптического диапазона, распространяемых через атмосферу.

Атмосферные оптические линии связи, а также комплексы, оборудования и системы в их составе, имеют целый ряд преимуществ:

* Высокая скорость передачи, обусловленная отсутствием сигнальной задержки между принятием и отправкой кадров, пакетов и сообщений данных;
* Низкая задержка в обработке кадров, пакетов и сообщений данных, обусловленная использованием в конструкции такого оборудования высокоскоростных печатных плат и высокочастотных электронных компонентов;
* Безопасность оптического канала, ввиду невозможности перехвата и расшифровки данных отправляемых и передаваемых с помощью инфракрасного оптического излучения;
* Свободное лицензирование по сравнению с радиочастотными и СВЧ-системами, для приобретения, установки и проведения пуско-наладочных работ которых требуется специальное разрешение государственного органа имеющего функции лицензирования в области специальных телекоммуникационных комплексов.

Одновременно с этим, атмосферные оптические линии связи, а также комплексы, оборудования и системы в их составе, имеют целый ряд недостатков:

* Высокая чувствительность к плохим погодным условиям ввиду того, что инфракрасный оптический сигнал не имеет эффекта усиления и разряженная атмосфера является дополнительным слоем сигнальных помех при передаче и отправке информации по атмосферным оптическим линиям связи;
* Ограниченная дальность атмосферных оптических линий связи, обусловленная наличием оптических линз в передающем и принимающей оптическом терминале;
* Влияние окружающей местности на характеристики сигнала, передаваемого по атмосферным оптическим линиям связи ввиду отражения сигнала от различных плоскостей.

Целью данной работы является проектирование, изготовление и отладка атмосферной оптической линии связи с использованием оптимизированных для микроконтроллерной архитектуры алгоритмов легковесной криптографии.

Для достижения данной цели необходимо решить следующие задачи:

* Исследовать принципы передачи информации с использованием атмосферных оптических линий связи;
* Исследовать принципы проектирования высокоскоростных печатных плат и высокочастотных элементов с использованием средств автоматизированного проектирования;
* Исследовать принципы проектирования программного кода для микроконтроллерных платформ с поддержкой аппаратных криптографических алгоритмов;
* Оптимизировать криптографический алгоритм для микроконтроллерной платформы, поддерживающей аппаратное ускорения криптографических алгоритмов;
* Создать стенд для реализации атмосферной оптической линии связи с поддержкой ускорения криптографических операций для шифрования информации передаваемой по инфракрасному оптическому каналу связи.

# АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

## Передача информации в открытом пространстве

Атмосферные оптические линии связи (на англ. – Free Space Optics) в своей архитектуре передачи и приема информации используют оптические инфракрасный сигнал в качестве канала связи с использованием оптических линз для корректировки конечной либо начальной точки передач и приема информации.

Аппаратно-программные комплексы, использующиеся для передачи и приема информации по атмосферным оптическим линиям связи имеют иное строение ввиду необходимости принимать, генерировать и корректировать инфракрасный оптический сигнал с использованием полупроводниковых лазерных диодов (Рисунок 1).



Рисунок 1 – Оптический инфракрасный трансивер, используемый для передачи и приема информации по атмосферной оптической линии связи

Структурная схема передачи информации по атмосферным оптическим линиям связи между аппаратно-программными комплексами имеет следующий вид (Рисунок 2).

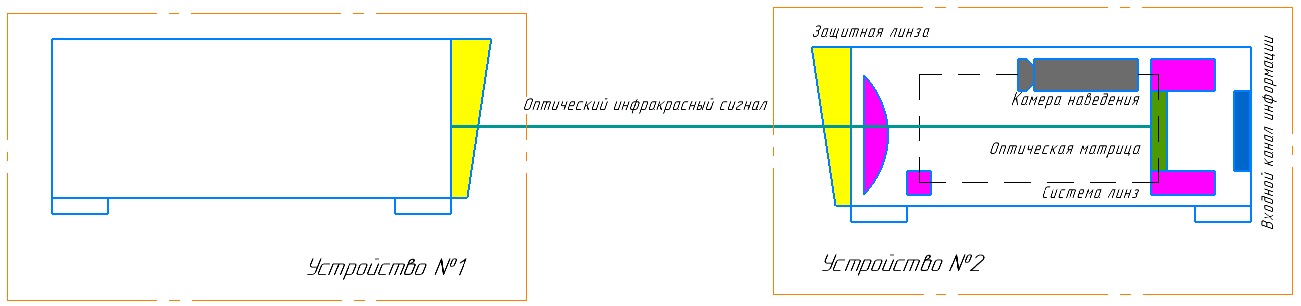


Рисунок 2 – Структурная схема устройства №1 (передатчик) и устройства №2 (приемник) для передачи и приема сообщения по атмосферным оптическим линиям связи

Аппаратно-программные комплексы, использующиеся для передачи и приема информации по атмосферным оптическим линиям связи в своем составе, имеют следующие конструктивные элементы, которые прямо влияют на конечные характеристики передачи и приема информации:

* Защитная линза – набор диоптирических линз образующих единую оптическую систему для уменьшения искажения передаваемого и принимаемого сигнала;
* Камера наведения – устройство использующее в своем составе цифровую камеру и датчик расстояния необходимый для автоматического наведения передающего устройства в область видимости принимающего устройства;
* Система линз – набор транспарентных линз образующих единую оптическую систему для компактного преобразования инфракрасного оптического сигнала;
* Оптическая матрица – интегральная микросхема с оптическим выходом, на входе принимающая инфракрасный оптический сигнал собранный с помощью системы линз;
* Входной канал информации – блок печатных плат и электронных дискретно-аналоговых компонентов преобразующих инфракрасный оптический сигнал собранный с помощью оптической матрицы в последовательной цифрового сигнала;

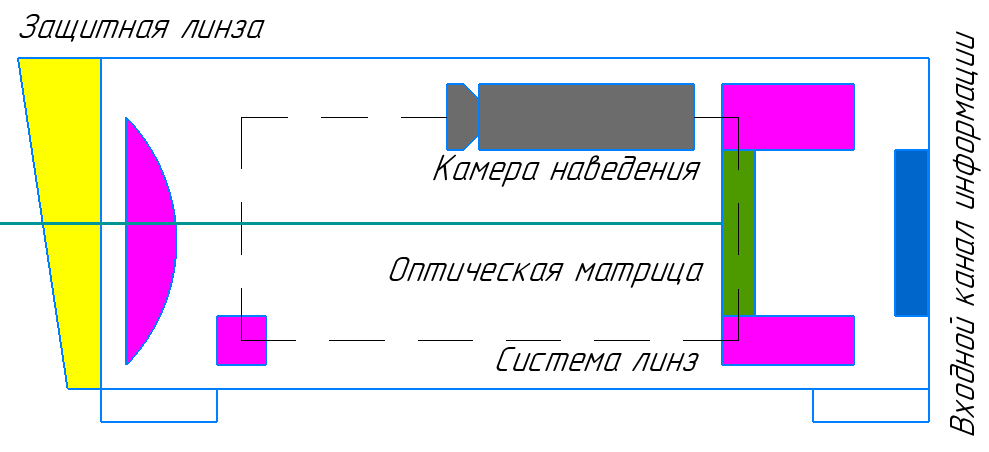


Рисунок 3 – Конструкция устройства для передачи и приема сообщения по атмосферным оптическим линиям связи

## Описание целей разработки

Использование преимуществ торговой площадки в интернет можно продемонстрировать с помощью SWOT-анализа.

Такая технология дает возможность не только определить проблемы, которые мешают росту продаж, но и выявить пути, предполагающие поиск тенденций развития компании, использующей интернет-магазин как площадку для продвижения.

## Анализ существующих технологий передачи информации в открытом пространстве

Учитывая тот факт, что интернет-магазин достаточно сложная система и предполагает не только сам процесс продажи и представления товара, необходимо использование и других нотаций, отражающих иные процессы, например, регистрацию пользователей интернет-магазина. Так как пользователь получает большее число функций в процессе оптимизации.

## Обоснование проектных решений

Набор инструментов и технологий разработки веб-представительств или интернет-магазинов, можно разделить на четыре основные группы:

* шаблонные решения, функционал которых заранее определен и ограничен возможностями предоставленными разработчиками или хостерами бесплатно, или на правах аутсорсинга в рекламных целях;
* комплексные системы управления содержимым, предполагающие определенный набор инструментов для работы с веб-контентом;
* интеграционные решения, включающие платформы работы с контентом и технологии работы с базами данных информационной системы предприятия;
* проекты на основе базы данных и интерфейсного сценарного языка для динамических сайтов ([Java](https://ru.wikipedia.org/wiki/Java), [PHP](https://ru.wikipedia.org/wiki/PHP), [Perl](https://ru.wikipedia.org/wiki/Perl), [ASP.NET](https://ru.wikipedia.org/wiki/ASP.NET), [Ruby](https://ru.wikipedia.org/wiki/Ruby)) с использованием фреймворков.

1. ПРОЕКТИРОВАНИЕ АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКСА
   1. Проектирование аппаратного обеспечения комплекса

Современное развитие информационно-коммуникационных технологий предъявляет к разработке аппаратного обеспечения все больше автоматизированных средств проектирования. Проектирование аппаратного обеспечения невозможно без определения цели устройства, его электронных компонентов, печатной платы и электрической принципиальной схемы.

Проектирование аппаратного обеспечения выполняется в системах автоматизированного проектирования специального назначения (на англ. Electronic design automation) для размещения, трассировки и соединения электронных устройств, компонентов и сигнальных дорожек.

Системы автоматизированного проектирования, предназначенные для проектирования электронных устройств, печатных плат и микросхем имеют свои различия и сходства. Главная задача таких систем автоматизированного проектирования заключается в изначально правильном проектировании электронных устройств и изделий для последующей передачи конструкторско-чертежной документации на производство и организации процесса промышленного производства спроектированного устройства [2].

Системы автоматизированного проектирования, предназначенные для проектирования электронных устройств, печатных плат и микросхем различаются по имеющемуся функционалу, лицензирования и наличию интегрированной среды математического и физического моделирования, что бывает полезно при проектирование комплексных устройств и систем высокой топологии (Таблица 1).

Таблица 1 – Сравнение САПР для проектирования печатных плат

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Класс** | **САПР** | **Описание** |
| **1** | *Любительские* | KiCAD | Бесплатная САПР для разработки электронных схем и печатных плат легкой и средней сложности без возможности моделирования |
| EagleCAD | Платная САПР для разработки электронных схем и печатных плат легкой и средней сложности без возможности моделирования |
| **2** | *Полупрофессиональные* | Altium Designer | Платная САПР для проектирования электронных схем и печатных плат средней и высокой сложности с удобным интерфейсом и большим набором функций |
| P-CAD | Платная САПР для проектирования электронных схем и печатных плат высокой сложности, предназначенная для работы с многослойными платами |
| Proteus | Платная САПР для проектирования электронных схем и симуляции работы устройств |
| **3** | *Профессиональные* | Mentor Graphics PADS | Платная САПР для проектирования электронных схем и печатных плат, предназначенная для работы с многослойными платами и высокочастотными сигналами |
| Cadence Allegro | Платная САПР для проектирования электронных схем и печатных плат, предназначенная для работы с многослойными платами и высокочастотными сигналами. |
| ANSYS Electrics Suite | Платная САПР для проектирования электронных схем и моделирования работы устройств в условиях высоких частот и электромагнитных помех |

Дальнейшее проектирование устройства, печатной платы, а также трассировка дорожек и размещения компонентов при помощи программного комплекса САПР от компании Cadence Design System, USA:

1. Среда разработки и проектирования печатной платы – *Cadence Allegro 17.4* (см. Рисунок 3).
2. Среда анализа и моделирования печатной платы – *Cadence Sigrity 2019* (см. Рисунок 4).

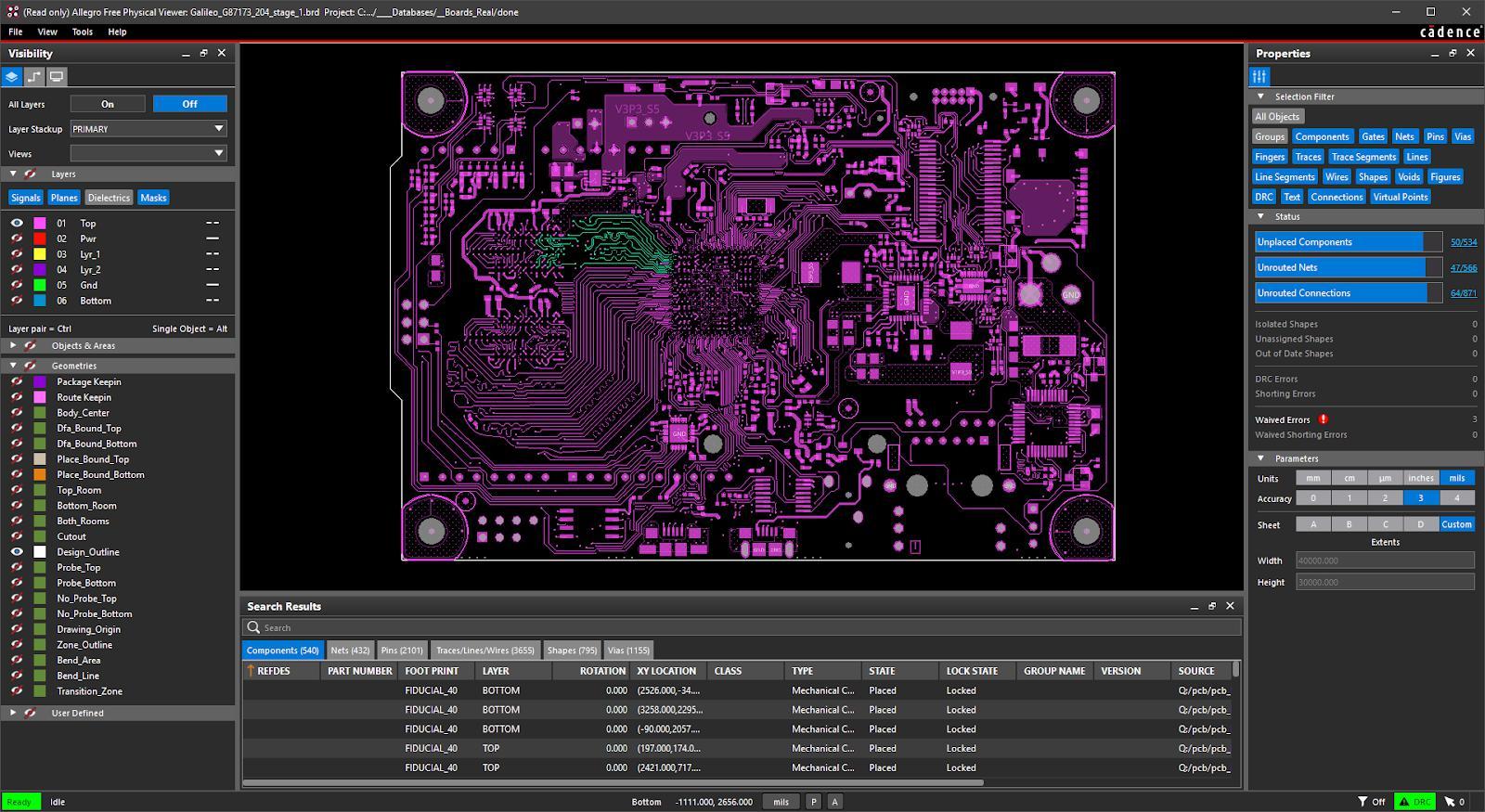


Рисунок 3 – Внешний вид Cadence Allegro PCB Designer 17.4

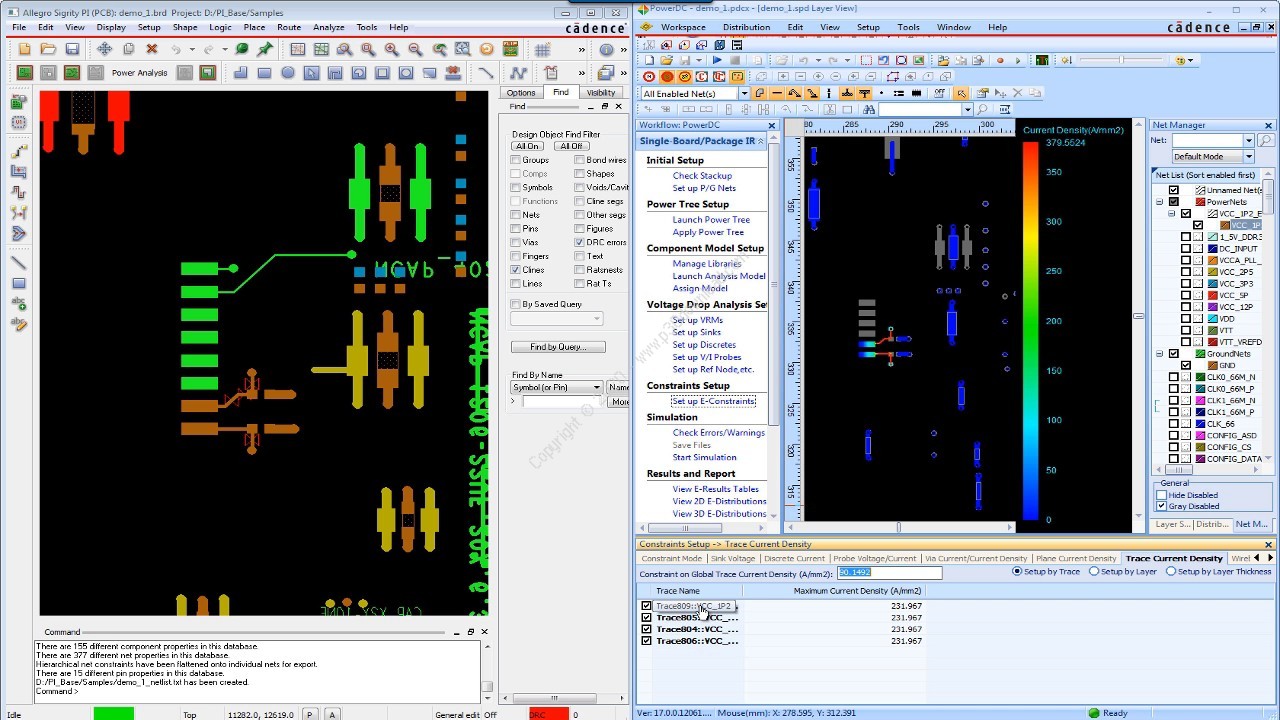


Рисунок 4 – Внешний вид Cadence Sigrity 2019

*Cadence Allegro 17.4* – профессиональная САПР для проектирования печатных плат и узлов высокой сложности и топологии, включает в себя программы для проектирования электрических принципиальных схем, топологии печатных плат, создания корпусов микросхем и простейшего анализа цепей питания и сигнальной передачи информации [3].

Проектирование, разработка и создание устройств производится в Cadence Allegro17.4. Данная САПР обладает принципом модульности и взаимозаменяемости, поэтому системное проектирование устройства производится в следующих программах входящих в САПР Cadence Allegro 17.4: [1]

1. Allegro Design CIS – программа для проектирования электрических принципиальных схем и создания электрических цепей с использованием компонентов доступных в интегрированных библиотеках (см. Рисунок 5).
2. Allegro PCB Designer – программа для проектирования печатной платы на основе уже созданной виртуальной модели устройства созданной на основе электрических цепей с использованием компонентов доступных в интегрированных библиотеках (см. Рисунок 6).

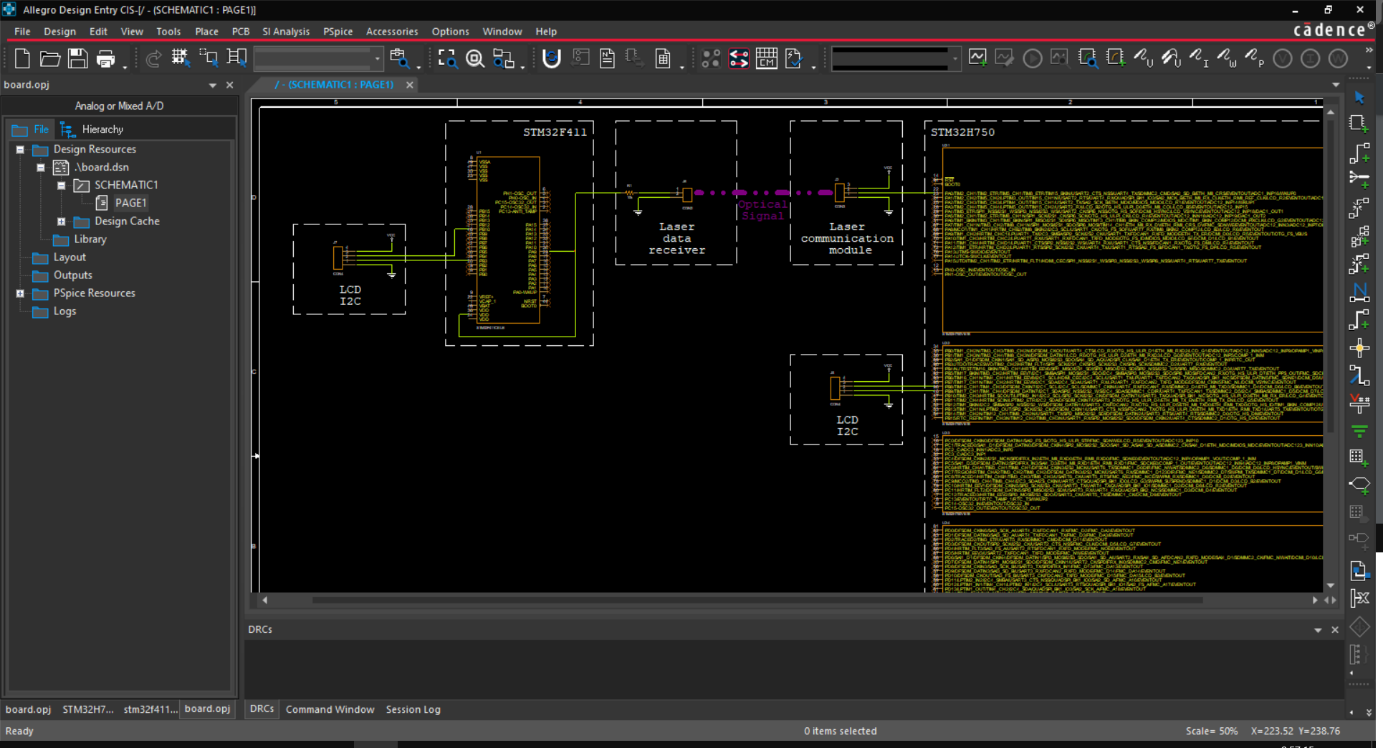


Рисунок 5 – Электрическая схема устройства спроектированная в Cadence Allegro Design CIS

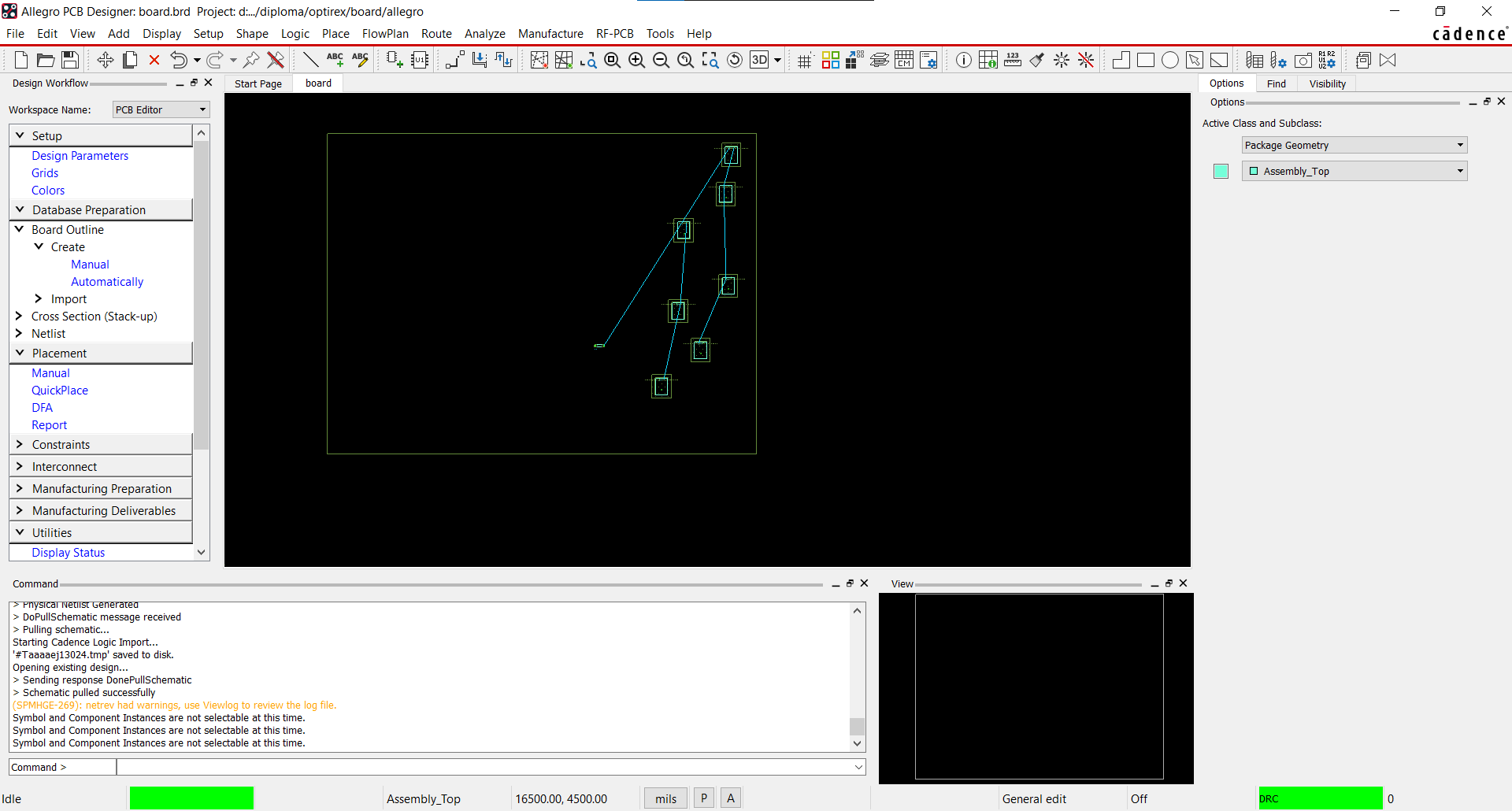
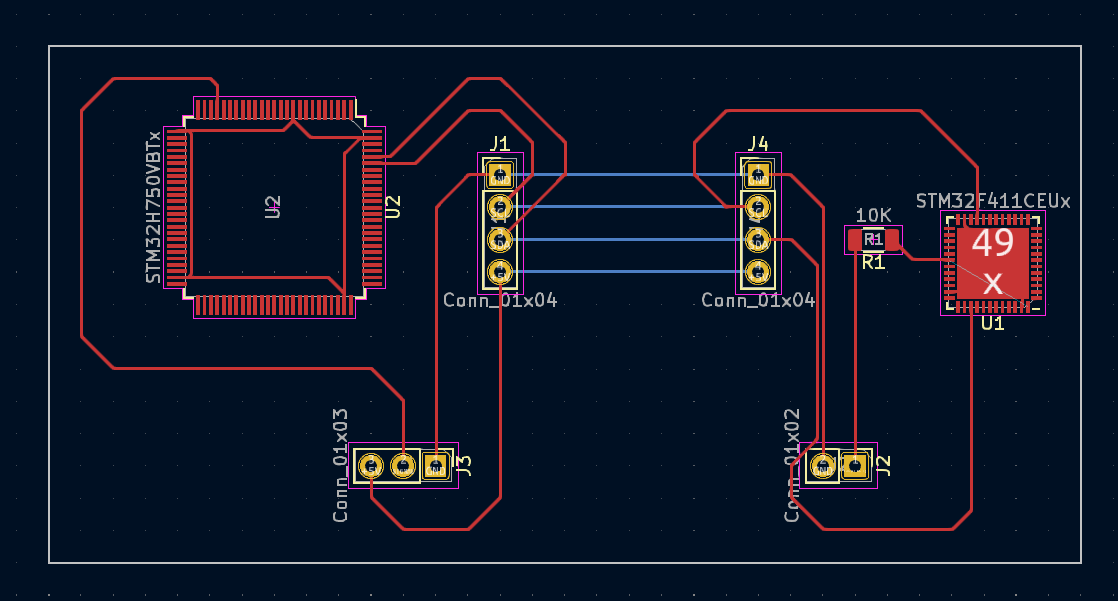


Рисунок 6 – Печатная плата на основе созданной электрической схемы Cadence Allegro PCB Designer

*Печатная плата* – (на англ. Printed Circuit Board) это пластиковая или фибростеклянная прямоугольная плата, которая содержит в себе составные компоненты, закрепленные в металлизированных отверстиях печатной платы. Между металлизированными отверстиями проводится трассировка дорожек согласно спроектированной электрической принципиальной схеме устройства или изделия. Развитие технологий создания печатных плат привели к тому, что печатные платы стали классифицироваться по топологической карте или количеству слоев):

* *Однослойная печатная плата* – печатная плата такого типа является самым распространенным типом и позволяет в домашних условиях производить печатные платы такого типа, например печатная плата для электронных часов или будильника.
* *Многослойная печатная плата* – печатная плата такого типа имеет несколько слоев проводников, разделенных диэлектрическим слоем, что позволяет размещать большое количество компонентов на одной печатной плате и таким образом уменьшить габариты печатной платы, например – печатная плата для оптических трансиверов или светодиодных ламп (см. Рисунок 1).
* *Высокоскоростная печатная плата* – печатная плата такого типа имеет особые требования к дизайну и материалам, чтобы обеспечить быстрый переход сигнала через проводники и минимизировать потери сигнала во времени, например – материнская плата компьютера или одноплатный компьютер (см. Рисунок 2).
* Высокочастотная печатная плата – печатная плата такого типа имеет самые строгие требования к дизайну и материалам, чтобы обеспечить электромагнитную стабильность и совместимость высокочастотных компонентов, расположенных на печатной плате, например – SDR-приемник, эхолокаторы и различные телекоммуникационные комплексы.

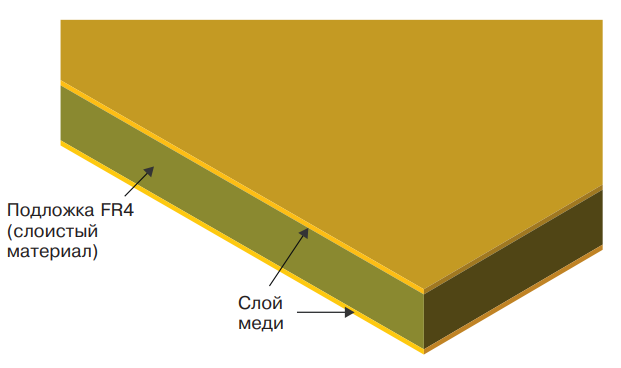
****

Рисунок 1 – Топология двухслойной печатной платы

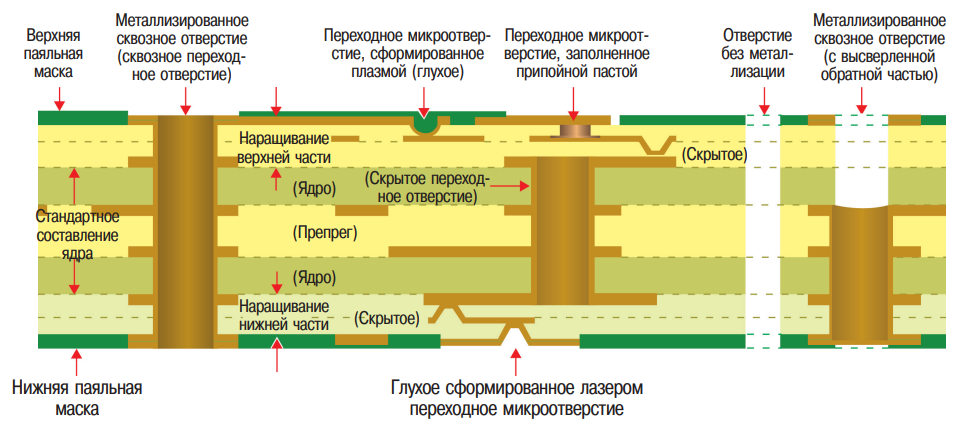
****

Рисунок 2 – Топология многослойной печатной платы

На сегодняшний день, любое современное электротехническое устройство или изделие содержит в себе многослойную печатную плату. В зависимости от роли устройства или изделия, компоненты на печатной плате могут различаться по типу, пакету, форм-фактору, расположению и монтажу.

В соответствии с моей темой выпускной квалификационной работы, принцип устройства заключается в следующем алгоритме:

* Шаг 1. Включение устройства №1 и устройства №2, приёмник и передатчик сигнала.
* Шаг 2. Определение и поиск оптической волновой активности с помощью программной проверки доступа оптического сигнала.
* Шаг 3. Шифрование информации с помощью алгоритма AES-128/192/256 на устройстве №1.
* Шаг 4. Передача зашифрованной информации на устройство №2.
* Шаг 5. Расшифровка информации на устройстве №2 в соответствии с уже загруженными ключами шифрования информации.
* Шаг 6. Вывод принятой информации на жидкокристаллический дисплей.

Цель устройства №1 и устройства №2 - выяснить практическим способом жизнеспособность теории о передачи зашифрованной информации по оптическому инфракрасному сигналу с использование микроконтроллеров и встроенных алгоритмов шифрования. При проектировании устройства (см. Рисунок 5) были использованы следующие компоненты (см. Таблица 2):

Таблица 2 – Список компонентов для устройства №1 и №2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Имя** | **Количество** | **Шелкография** | **Корпус** |
| **1** | CON2 | 7 | CON2n | Header\_Pin\_2.54mm |
| **2** | R, 10K | 1 | R1 | 1206\_SMD |
| **3** | U1 | 1 | STM32F411CEU6 | QFN50 |
| **4** | U2 | 1 | STM32H750VBT6 | QFN100 |
| **5** | KY-008 | 1 | LDR | Pin\_2.54mm |
| **6** | PHRES | 1 | PHRES | Pin\_2.54mm |

**1.2. Моделирование реальных условий работы высокоскоростной печатной платы**

*Cadence Sigrity 2019* – профессиональная среда анализа и моделирования печатных плат и узлов высокой сложности, включает в себя программы для анализа и моделирования печатных плат на термическую устойчивость, температурные перепады, электромагнитную и сигнальную совместимость (см. Рисунок 7) [1].

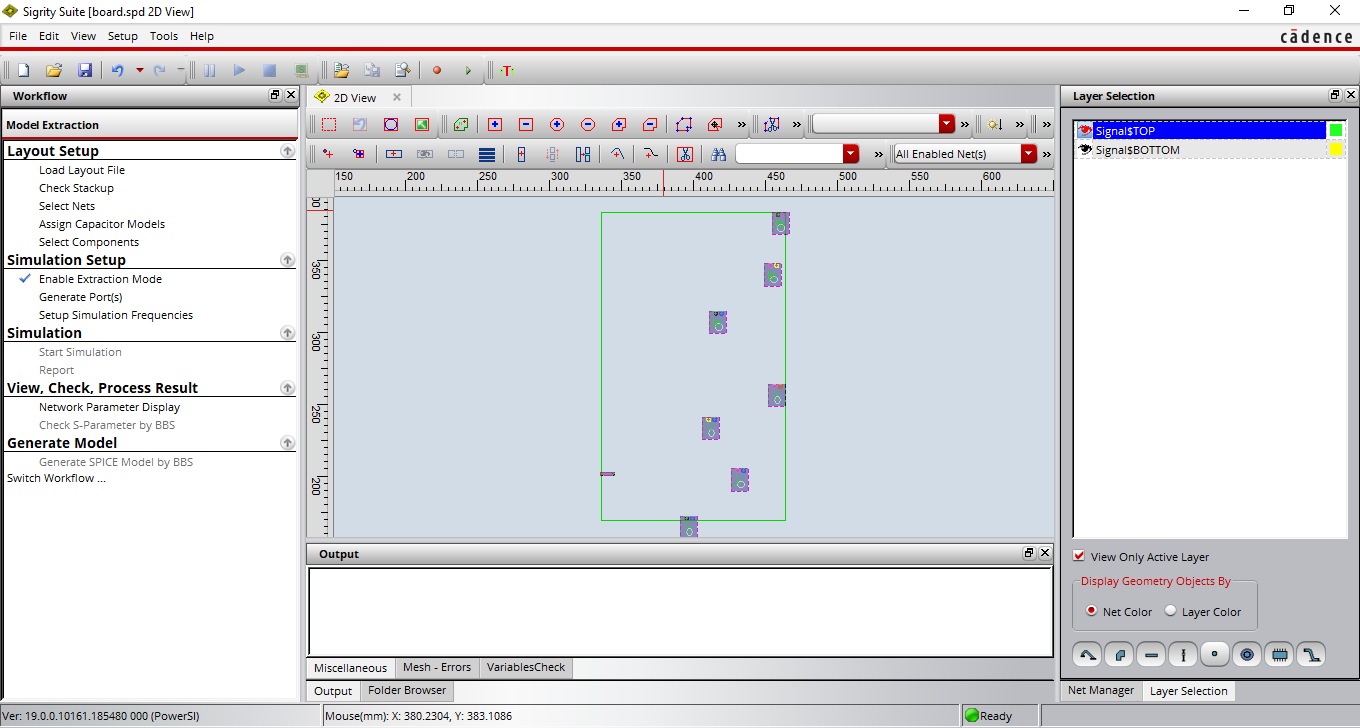


Рисунок 7 – Анализ печатной платы в Cadence Sigrity 2019 PowerSI

Утилита PowerSI входящая в состав среды анализа и моделирования печатных плат Cadence Sigrity 2019 провела анализ печатной платы и обнаружила следующие недостатки и конструктивные особенности первой версии печатной платы:

1. Топология электрических дорожек и проводников выведена неправильно и не позволяет корректно смоделировать реально поведение устройства в среде моделирования [1].
2. Создания конденсационного электромагнитного поля на участках электрических цепей в местах подключения оптических трансиверов и ресиверов [1].
3. Вычислительные устройства передачи данных – микроконтроллеры имеют высокое сигнальное поле и должны быть расположены либо отделены от остальной части печатной платы слоем диэлектрических дорожек, либо сигнально-диэлектрическим слоем внутри, либо на верхнем слое печатной платы [1].

Параллельно с этим, мною был проведен собственный анализ печатной платы, которая была выпущена опытно-промышленной серией в одну единицу с помощью фоторезистивной технологии переноса топологии печатной платы на стеклотекстолит FR4 с применением защитного сигнального слоя (см. Рисунок 8 и 9).

Моделирование печатной платы с помощью программного пакета Cadence Sigrity 2019 показало недостатки и различные конструктивные ошибки допущенные в процессе проектирования печатной платы и опытно-промышленного выпуска в одну единицу (см. Рисунок 10).

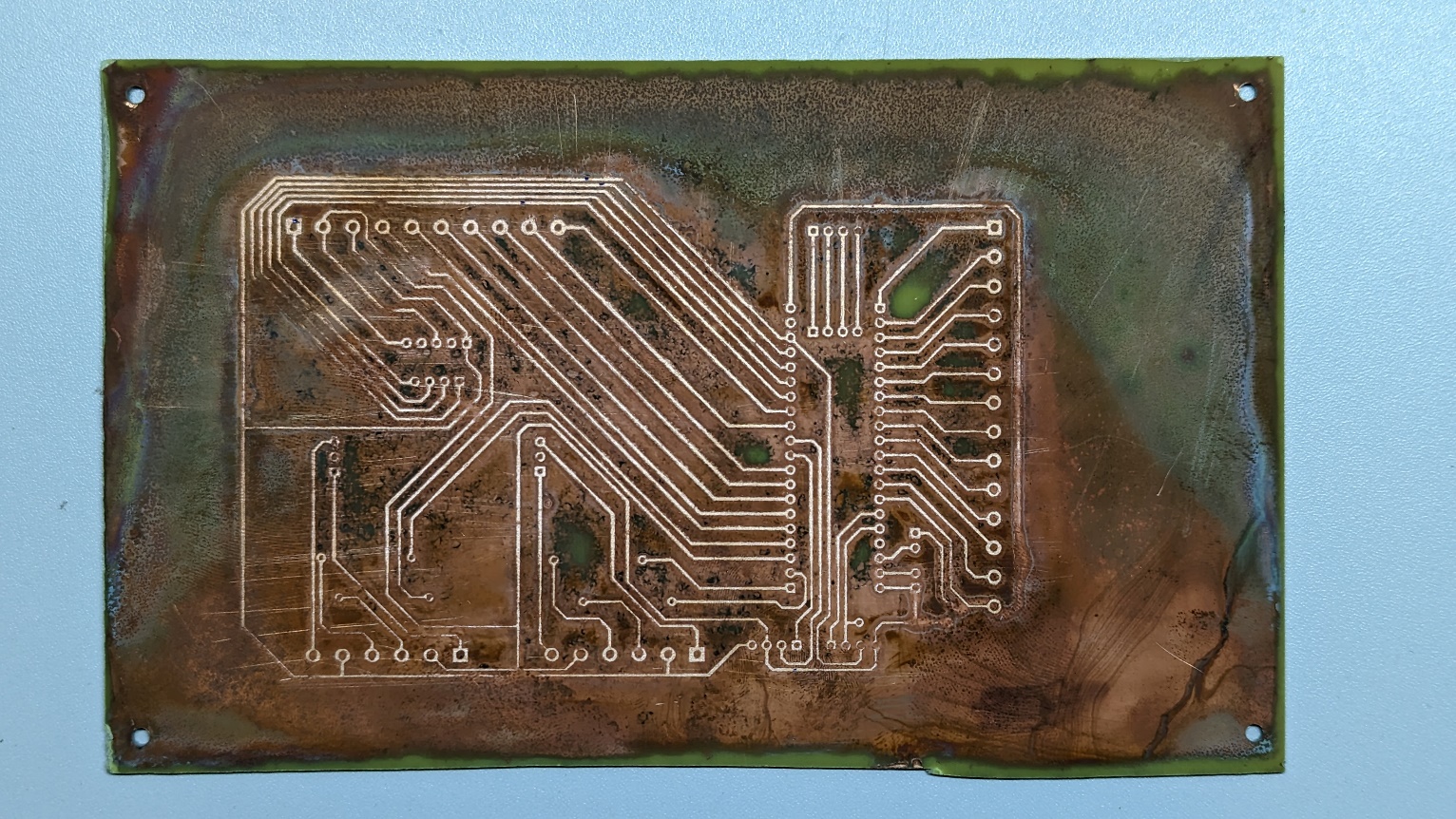


Рисунок 10 – Первая версия печатной платы устройства

После опытно-промышленного выпуска печатной платы устройства в количестве одной единицы были выявлены следующие недостатки и конструктивные особенности печатной платы:

1. Печатная плата под воздействием высоких температур или температурных перепадов имеет свойство окисления и создания «защелок» непосредственно на электрических цепях устройства №1 и №2.
2. Топология электрических дорожек и соединений имеет неправильную форму, непригодную для применения в опытно-промышленной версии устройств.
3. Подключение микроконтроллеров и датчиков лучше сделать внешним из-за несогласованности частотного импеданса между оптическими и электрическими компонентами.
4. Микроконтроллер и его компоненты влияют на согласованность передачи информации по оптическому каналу связи между устройствами №1 и №2.
5. Создание второй версии печатной платы потребует ухода от фоторезистивной технологии в пользу аутсорсинга производства печатной платы другими фирмами и компаниями.
   1. Проектирование программного обеспечения комплекса

Разработка встраиваемых приложений для микроконтроллеров серии STM32, осуществляется с помощью интегрированной среды разработки STM32CubeIDE (см. Рисунок 11) компании STMicroelectornics с бесплатной лицензией и пожизненным сроком обновления и сервисной поддержки.

Рисунок 11 – Основные этапы разработки приложения для встраиваемых систем

В составе STM32CubeIDE есть также специальное программное обеспечение STM32CubeMX, служащее для упрощения программирования и проведения первоначальной настройки микроконтроллера. Основным преимуществом данной среды разработки является то, что благодаря специальному хранилищу, при подключенном интернете, пользователь имеет доступ ко множеству библиотек и примеров внутри интегрированной среды разработки.

Основное пространство пользовательского интерфейса занимает текстовый редактор кода, в нем пользователь создает приложения на встраиваемых систем на языках программирования C и C++. В текстовом редакторе присутствует система проверки типов и ошибок. Также имеется очень удобная система авто дополнения программного кода, основанная на частотном анализе наиболее используемых функций, которая, при написании некоторой последовательности символов, предлагает разработчику дополнить программный код, чтобы получить необходимые функции микроконтроллера.

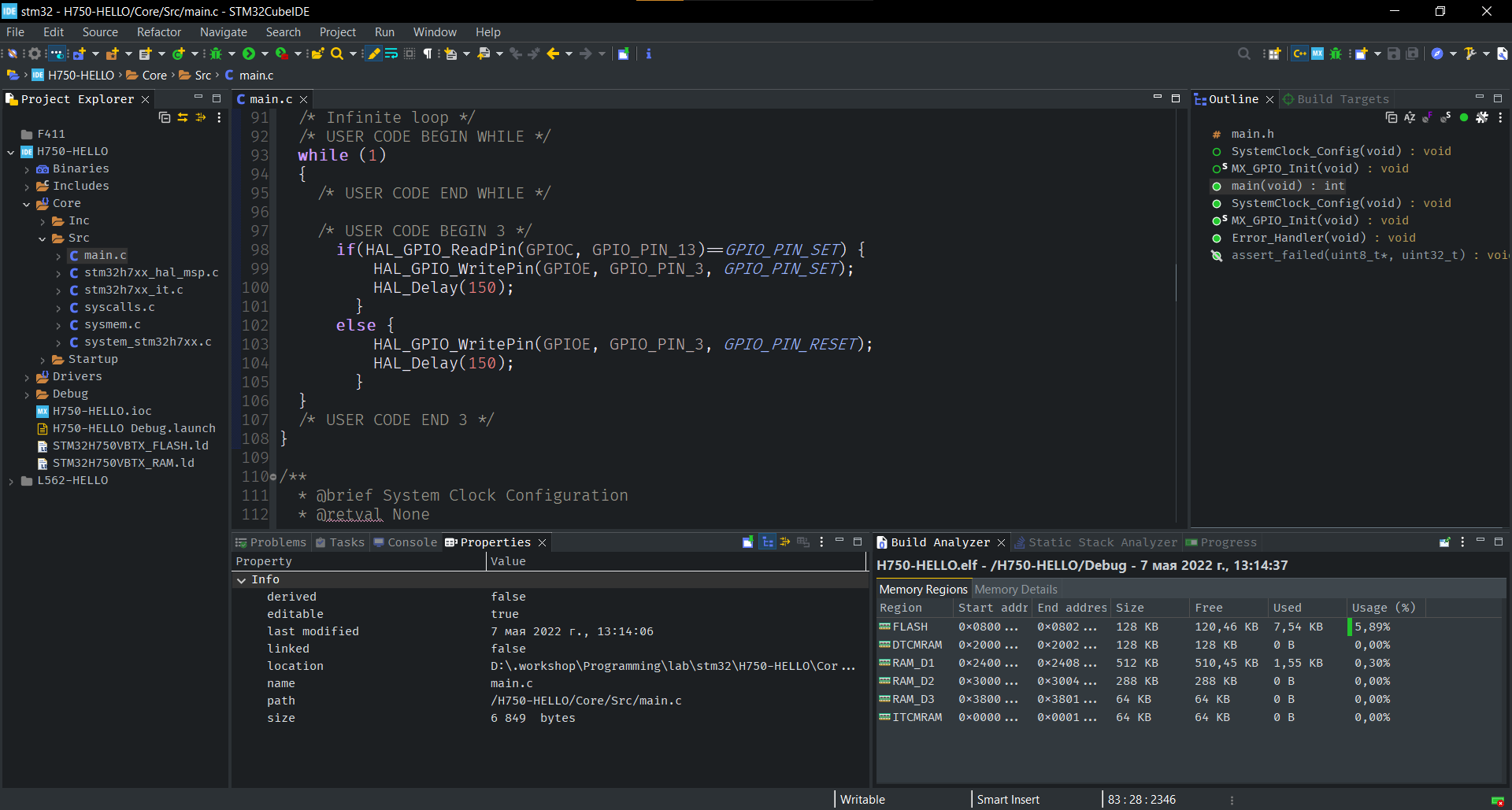


Рисунок 12 – Разработка и отладка программного кода встраиваемых систем на основе микроконтроллера ARM промышленного стандарта с использованием IDE STM32CubeIDE

STM32CubeIDE сочетает в себе несколько утилит, необходимых для правильной первоначальной настройки и программирования микроконтроллеров STM32, а именно:

* *STM32CubeMX* – проводит первоначальную настройку микроконтроллера и дает возможность использовать внешние и внутренние интерфейсы микроконтроллера;
* *STM32CubeProgrammer* – проводит глубокую настройку микроконтроллера, а также позволяет в реальном времени следить за основными характеристиками микроконтроллера;
* *STM32CubeMonitor* – проводит анализ всей встраиваемой системы с помощью внешних и внутренних датчиков;

В качестве итога, можно сказать, что разработка приложений для встраиваемых систем, стала намного более удобной, одновременное с этим появилось множество дополнительных утилит при работе с такими системами, которые качественно улучшают продуктивность и качество разработки программного кода для встраиваемых систем [6].

Первоначальная разработка программного кода производилась на основе работы с программируемым учебным стендом «MPS-2.1» выполненной на основе микроконтроллера STM32F103C8T6. Стенд учебный программируемый «MPS-2.1» (см. Рисунок 13 и 14) представляет собой компактное устройство, выполненное из ударопрочного пластика включающее в себя большое количество различных модулей. Устройство моделирует работу основных систем современного легкового автомобиля. Стенд позволяет создавать различные конфигурации программ приближенных к используемым в транспортных, роботизированных и мехатронных системах различной специализации [7].

Устройство обладает рядом достоинств:

* мобильность;
* возможность использования устройства в автономном режиме и от сети;
* защита от некорректных действий;
* изолированный ударопрочный корпус;
* простота замены отдельных модулей;
* возможность визуального наблюдения за работой модулей.

|  |  |
| --- | --- |
|  |  |
| Рисунок 13 и 14 – Общий и инженерный вид стенда учебного программируемого MPS-2.1 | |

Таблица 3 - Технические характеристики MPS-2.1

|  |  |
| --- | --- |
| **Параметр** | **Значение** |
| Размеры (ШхВхГ) (без учета колес) | 160х83х210 мм |
| Размеры (ШхВхГ) (с учетом колес) | 220х83х210 мм |
| Масса | 800 гр. |
| Рабочая температура | 10-35 С° |
| Рабочее напряжение | 7-10 В |
| Напряжение питания адаптера | 220 В |
| Максимальная скорость вращения колёс | 300 об/мин |
| Максимальный ток адаптера | 3 А |
| Напряжение на выходе адаптера | 9 В |
| Тип аккумуляторов | Li-Ion стандарта 18650 |
| Количество аккумуляторов | 2 шт. |
| Количество символов дисплея LCD2004 | 20х4 |
| Количество символов дисплея TM1637 | 4 |

Основой устройства является STM32F103C8T6 (см. Рисунок 15) — это микроконтроллер, построенный на ядре ARM Cortex-M3. Данное ядро имеет много преимуществ, но его основное преимущество на сегодняшний день — универсальность. За годы существования ядра Cortex-M3, он стал индустриальным и промышленным стандартом. Об этом говорит количество производителей, присоединившихся к данной архитектуре и количество выпущенных устройств на базе данного микроконтроллера [5].

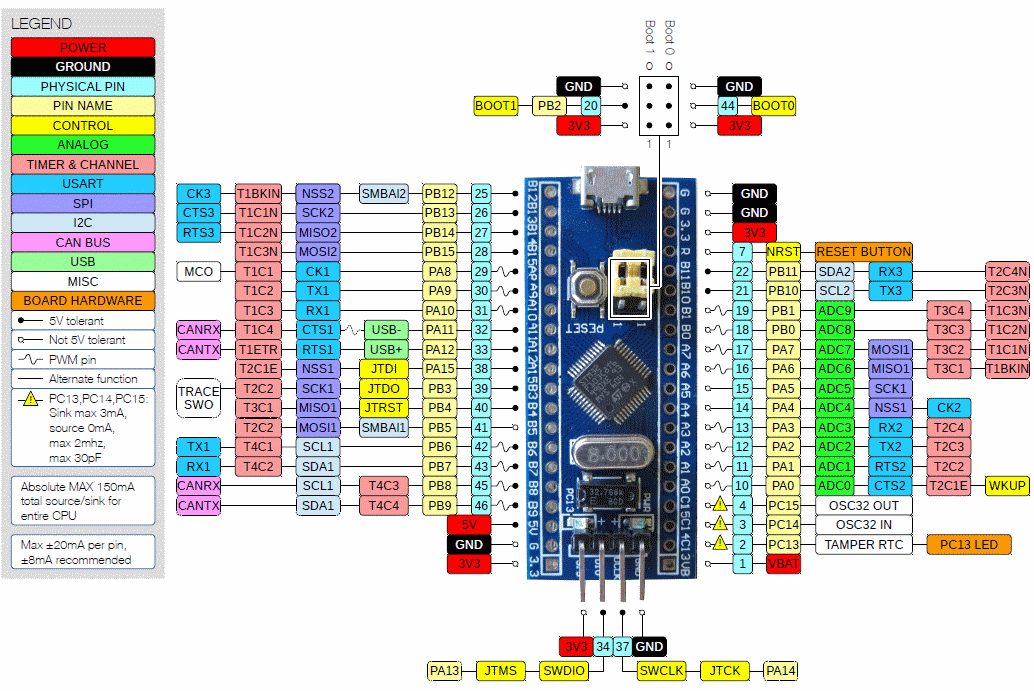


Рисунок 15 – Микроконтроллер STM32F103C8T6

Таблица 4 – Технические характеристики микроконтроллера STM32F103C8T6

|  |  |
| --- | --- |
| **Параметр** | **Значение** |
| Разрядность микроконтроллера | 32 бита |
| Максимальная частота | 72 МГц |
| Объем памяти программ (FLASH) | 64 кбайт |
| Объем памяти данных (RAM) | 20 кбайт |
| Общее количество входов/выходов | 37 |
| Количество таймеров общего назначения | 3 |
| Количество расширенных таймер с ШИМ-коррекцией управлением двигателя | 1 |
| Системный таймер | 1 |
| Сторожевые таймеры | 2 |
| Количество интерфейсов UART | 3 |
| Количество интерфейсов SPI | 2 |
| Количество интерфейсов I2C | 2 |
| Количество интерфейсов CAN | 1 |
| Количество интерфейсов USB | 1 |
| Контроллеры прямого доступа к памяти | 7 |
| Наличие АЦП/ЦАП | АЦП 10x12b |
| Часы реального времени | есть |
| Аппаратный модуль расчета CRC | есть |
| Напряжение питания микроконтроллера | от 2 до 3,6 В |
| Напряжение питания платы | 5 В |
| Ток потребления | до 50 мА |
| Размеры платы | 53 x 22,5 мм |

Семейство STM32 отличается от конкурентов хорошим поведением в температурном диапазоне от -40 до 85°С. Производительность ядра и периферии сохраняется полностью. В семействе STM32 есть ряд изделий, сертифицированных на расширенный температурный диапазон от -40 до 105°С [4].

Одна из причин мировой популярности семейства STM32 — максимальный комфорт разработчика. Если универсальность ядра STM32 позволяет менять производителя c минимальными затратами на программный код, то Pin-to-Pin совместимость внутри семейства STM32 позволяет менять объем памяти (флэш-память и ОЗУ) и периферию (Ethernet, USB, CAN, и т.д.), не трогая печатную плату. «Pin-to-Pin совместимость» означает, что для одного размера корпуса все сигналы сохраняются на тех же самых вводах/выводах для разных вариантов микроконтроллеров семейства.

3. ОПТИМИЗАЦИЯ КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА

3.1. Криптографический алгоритм AES

В период с 1972 по 1977 года в ходе открытого конкурса и общественных слушаний по созданию криптографического алгоритма устойчивого к криптоанализу и различным атакам, Национальным бюро стандартизации Соединенных Штатов Америки был принят в качестве финального алгоритма – криптографический алгоритм DES (Data Encryption Standard, с англ. – стандарт шифрования данных), разработанный компанией IBM.

Архитектура алгоритма DES основывалась на использовании принципов симметричного шифрования информации – использовании блоков открытого и секретного текста. Блоки открытого и секретного текста имели размерность в 64 бита каждый, при этом длина ключа необходимого для совершения операции шифрования и расшифрования информации первоначально составлял 56 бит.

Алгоритм DES основан на использовании ячеек Фейстеля и таблиц расширения с возможностью перестановки битов текста. Использовании архитектуры сети Фейстеля с возможностью раундовой обработки текста позволило существенно уменьшить зависимость от прямого криптоанализа и имело преимущество в виде аппаратной реализации криптографического алгоритма с помощью логических интегральных микросхем.

Для повышения стойкости криптографического алгоритма и замены стандарта DES, в 1997 был объявлен открытый конкурс по созданию криптографического алгоритма устойчивого к атаке «грубой силой». Алгоритм DES кроме неоспоримых преимуществ имел фундаментальные недостатки, заложенные еще при разработке и имплементации криптографического алгоритма, а именно:

* Невозможность использовать поточное шифрование информации;
* Длина ключа в 56 бит позволяла со временем реализовать атаку методом «грубой силы», при которой возможно осуществить полный перебор всех ключей необходимых для шифрования информации на всех этапах передачи по линиям связи.

3.2. Аппаратные ускорители шифрования и дешифрования информации

Чтобы покупатель перешел на страницу электронного магазина, ему необходимо ввести URL сайта. Вся навигация происходит через главное меню, компонентами которого являются: Главная; О Магазине; Платеж и Доставка; Покупка в кредит; Новости; Информеры; Товар; Корзина; Контакты; Авторизация; Регистрация и Каталог [1, 2].

3.3. Оптимизация криптографического алгоритма AES

Руководство пользователя — это документ, содержащий инструкции по установке, использованию или устранению неполадок аппаратного или программного продукта [3, 4]. Руководство пользователя может быть очень кратким - например, всего 10 или 20 страниц, или это может быть полная книга объемом 200 или более страниц. Хотя это определение предполагает использование компьютеров, руководство пользователя может содержать инструкции по эксплуатации практически для всего: газонокосилки, микроволновые печи, посудомоечные машины и т. д.

ЗАКЛЮЧЕНИЕ

Актуальность информационных систем в сфере бизнеса не оспаривается. Все предприятия вкладывают огромные ресурсы в электронную коммерцию, тем самым создавая огромную конкуренцию друг другу.

Актуальность информационных систем в сфере бизнеса не оспаривается. Все предприятия вкладывают огромные ресурсы в электронную коммерцию, тем самым создавая огромную конкуренцию друг другу.

Разработанная электронная структура повышает эффективность управления за счет создания эффективной, ходовой и главное работающей единой базы данных.

В ходе выполнения данной работы была разработана электронная система «Интернет-магазин компьютерной техники», которая позволяет покупать компьютеры и комплектующие, в любое удобное для покупателя время.

В данной работе были построены и указаны диаграммы работы общей информационной структуры, диаграммы потока всех данных продемонстрированы все ходы создания общего интерфейса пользователя, все сценарии данной работы, отражающие логику всей системы.

Также была продумана и создана общая логическая схема. Для реализации данной работы мы использовали диаграммы классов между классами.

С нуля была построена современная и работающая Графа Диалога, указывающая все пути навигации нашего веб-проекта.

Целью в данной работе предлагалось расширить границы бизнеса предприятия

TOO «EasyComp» за счёт создания и поддержки веб-сайт, содержащего информацию о предприятии, его услугах, и непосредственно сам интернет-магазин по продаже техники.

Для реализации данного проекта был выбран язык PHP, а в качестве СУБД – пакет MySQL. Для создания и редактирования всех интерфейсов были выбраны следующие программы:

* Wordpress;
* AdobePhotoshop;
* AdobeInDesign;

Было создано руководство пользователя, для навигации, а также возможности быстро отвечать на вопросы целевой аудитории.

Цель данного дипломного проекта достигнута – разработан проект web-сайта. Архитектура всего проекта была проверена, и мы можем с уверенностью заявить, что она работает.

Мы показали, что создание архитектуры с нуля позволяет понять, как устроена модель электронного магазина, какова его структура, свойства, законы моделирования; научиться управлять данной архитектурой, развивать ее в необходимом русле, определять наилучшие способы управления проектом, прогнозировать последствия тех или иных действии в данной модели проекта.

Суть разработки программы виртуального интернет-магазина позволяет дополнительно изучить аспекты маркетинга, бизнес-администрирования, и изучить многие тонкости веб-дизайна.

# СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. ГОСТ 34.601-90 Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
2. ГОСТ Р ИСО/МЭК 12207-99 Информационная технология. Процессы жизненного цикла программных средств.
3. ГОСТ Р 6.30-2003 Унифицированные системы документации «Унифицированная система организационно-распорядительной документации. Требования к оформлению документов».
4. ISO 15846, ISO 10007. Стандарты по менеджменту конфигурации программных средств.
5. Goldenberg B. J. The Definitive Guide to Social. Maximizing Customer Relationships with Social Media to Gain Market Insights, Customers, and Profit CRM. 2015 ISM, Inc. – 255 p.
6. Travagiliante R. WordPress from «A» to «W». – М.: Книга по требованию, 2017. – 324 с.
7. Бартлетт Д. Wordpress для начинающих. – М.: ЭКСМО, 2017. – 208 с.
8. Басыров Р. 1С-Битрикс. Постройте профессиональный сайт сами! – СПб.: Питер, 2017. – 120 с.
9. Долганов, О.И. Моделирование бизнес-процессов / О.И. Долганов, Е.В. Виноградова, А.М. Лобанова. – М.: Юрайт, 2016. – 290 с.
10. Маглинец Ю.А Анализ требований к автоматизированным информационным системам: Учебное пособие / Ю.А. Маглинец. – СПб.: Бином, 2015. – 200 с.
11. Робен Дж.Н. HTML5, CSS3 и JavaScript. Исчерпывающее руководство (+ DVD-ROM): учебник. – М.: Эксмо, 2014. – 528с.
12. Сергеев А. Создание сайтов на основе WordPress. Учебное пособие. – М.: Лань, 2015. – 128 с.
13. Сорокина М.В. Менеджмент в торговле: учебник для вузов. Стандарт третьего поколения. – СПб.: Питер, 2017. – 752 с.
14. Фримен Эл., Фриман Эр. Изучаем HTML, XHTML и CSS: учебник. – СПб.: Питер, 2016. – 720 с.
15. 1С: Битрикс. CMS система управления проектами [Электронный ресурс]. – 2019. <http://www.1c-bitrix.ru/> (дата обращения: 18.04.2020).
16. 1С-Битрикс. Управление сайтом [Электронный ресурс] – 2019. <https://www.1c-bitrix.ru/> (дата обращения: 18.04.2020).
17. CRM Битрикс24 [Электронный ресурс] – 2019. <https://www.bitrix24.ru/features/crm.php> (дата обращения: 18.04.2020).

1. [Laravel - The PHP Framework For Web Artisans](https://laravel.com/) [Электронный ресурс]. – 2019. https://laravel.com/ (дата обращения: 18.04.2020).
2. Software as a service Программное обеспечение как услуга. TAdviser [Электронный ресурс] – 2019 <http://www.tadviser.ru/index.php/SaaS> (дата обращения: 05.04.2020).
3. SQL Server. Microsoft [Электронный ресурс]. – 2019. <https://www.microsoft.com/ru-ru/server-cloud/products/sql-server/overview.aspx> (дата обращения: 18.04.2020).
4. Terrasoft. Продажи [Электронный ресурс] – 2019. <http://www.terrasoft.ru/sales/price> (дата обращения: 5.04.2020).

1. [Zend Framework: Home](https://framework.zend.com/) [Электронный ресурс]. – 2019. https://framework.zend.com/ (дата обращения: 18.04.2020).
2. Аналитический бюллетень inSales 2015: Рынок Интернет-торговли в России в 2014 году. [Электронный ресурс] – 2015. <http://www.insales.ru/blog/2015/05/20/analytical-bulletin-insales-2015/> (дата обращения: 3.04.2020).
3. Вpm’online service [Электронный ресурс] – 2019. <https://www.terrasoft.ru/service> (дата обращения: 5.04.2020).
4. Каталог CMS. [Электронный ресурс]. – 2019. http://www.cmsmagazine.ru/catalogue/ (дата обращения: 18.04.2020).
5. Кравченко В. [Клиентоориентированность и основные проблемы Топ-100 интернет-магазинов](http://www.searchengines.ru/articles/klientoorientir.html) [Электронный ресурс] – 2017. <http://www.searchengines.ru/> articles/klientoorientir.html (дата обращения: 3.04.2020).
6. Мегаплан. Клиенты и продажи [Электронный ресурс] – 2019. <https://megaplan.ru/crm/> (дата обращения: 17.04.2020).
7. НostCMS. [Электронный ресурс]. – 2019. http://www.hostcms.ru/ (дата обращения: 18.04.2020).
8. Отраслевые и специализированные решения [Электронный ресурс]. – 2019. [http://solutions.1c.ru/catalog/](http://solutions.1c.ru/catalog/restaurant/features) (дата обращения: 18.04.2020).
9. Попова М. Импортозамещающие СУБД: желания и возможности. // CNews. Аналитика. Обзор: Рынок ИТ: итоги 2014. [Электронный ресурс] – 2015. http://www.cnews.ru/reviews/2014/articles/importozameshchayushchie\_subd\_zhelaniya\_i\_vozmozhnosti (дата обращения: 18.04.2020).
10. Рейтинг систем управления базами данных (СУБД) 2016 // Tagline. Рейтинги сервисов и технологий [Электронный ресурс] – 2017 http://tagline.ru/database-management-systems-rating/ (дата обращения: 18.04.2020).
11. Среда разработки и система управления содержанием сайтов: Учебник [Электронный ресурс]. – 2019. <https://ru.wikibooks.org/wiki/MODx> (дата обращения: 18.04.2020).

1.1. Передача информации в открытом пространстве

1.2. Описание целей разработки

1.3. Анализ существующих технологий передачи информации в открытом пространстве

1.4. Обоснование проектных решений

ПРОЕКТИРОВАНИЕ АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКСА

2.1. Проектирование аппаратного обеспечения комплекса

2.2. Проектирование программного обеспечения комплекса

ОПТИМИЗАЦИЯ КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА

3.1. Криптографический алгоритм AES

3.2. Аппаратные ускорители шифрования и дешифрования информации

3.3. Оптимизация криптографического алгоритма AES