**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

Развитие высокотехнологичных отраслей экономики любого государства невозможно представить без комплексного развития системных компетенций, которые связывают между собой целые отрасли и разделы науки, образования, экономики и производства.

Информационно-коммуникационные технологии являются одним из основных факторов системного развития науки, образования и экономики любого государства. Развитие информационно-коммуникационных технологий с появлением телекоммуникационных комплексов создания принципиально новых способов передачи информации невзирая на количество передаваемых данных и условия окружающей среды.

Информационные системы, являясь вычислительным ядром информационно-коммуникационных технологий, отвечают за обработку и хранение различных данных. Особое значение информационные системы приобрели в государственных секторах экономики – структурах и органах безопасности, топливо-энергетических комплексах, финансовых организациях и других объектов хранящих конфиденциальную информацию. Информационные системы, обрабатывающие конфиденциальную информацию, входят в состав критической информационной инфраструктуры.

Особенность проектирования и обслуживания критической информационной инфраструктуры заключается в соблюдении принципа абсолютной информационной безопасности. Принцип абсолютной информационной безопасности предполагает, что на информационная система имеет максимальный уровень защиты от физического и информационного вектора атаки на объект критической информационной инфраструктуры, поскольку такие объекты хранят информацию и данные, утечка которых за периметр критической информационной инфраструктуры может привести к созданию новых векторов атаки на государственные органы и структуры.

При этом, в вопросе проектирования критической информационной инфраструктуры, особое внимание уделяется аппаратно-программным телекоммуникационным комплексам, имеющим интерфейсы для приема и передачи информации с внешним информационным полем. Современное развитие критической информационной инфраструктуры сочетает в себе использование различных типов телекоммуникационного оборудования – коммутационные и распределительные системы, спутниковые, оптические, волоконно-оптические, беспроводные и высокочастотные комплексы передачи и приема 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, критичных для некоторых условий работы в составе критической информационной инфраструктуры:

* 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 принципа передачи информации с помощью 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

Передача информации в телекоммуникационных системах зависит от типа используемой системы, топологии вычислительной сети, зоны действия и количества пользователей подключенных к вычислительной сети с помощью телекоммуникационных систем и комплексов. Телекоммуникационные системы по типу передачи сигналов делятся на несколько видов, и включают в себя следующие виды сигналов:

* аналоговый сигнал – телекоммуникационные системы, передающие информацию с помощью аналогово сигнала, имеют фундаментальные недостатки в виде невозможности шифрования передаваемой информации в потоковой форме, при этом такие системы имеют простую конструкцию;
* цифровой сигнал – телекоммуникационные системы, передающие информацию с помощью цифрового сигнала, имеют большую пропускную способность за счет использования бинарной логики при отправке и приеме сигнала, при этом в конструкции таких систем предполагается использование различного питания постоянного тока ввиду необходимости дифференциации различных сигналов;
* оптический сигнал – телекоммуникационные системы, передающие информацию с помощью оптического сигнала, имеют большую пропускную способность и сочетают в себе все преимущества аналоговой и цифровой передачи сигналов на дальнее расстояние, при этом такие системы в своей конструкции используют дорогостоящие оптические системы и линзы для корректировки и автоматической наводки оптического сигнала на устройство-приемник;
* беспроводной сигнал – телекоммуникационные системы, передающие информацию с помощью беспроводного сигнала, имеют в своем составе радиочастотный трансивер которые позволяет передавать сигнал на большее расстояние, и в зависимости от ширины канала передачи данных, радиочастотный трансивер имеет большую частоту и амплитуду сигнала, что влечет за собой дополнительное тепловыделение и генерацию постороннего шума.

Атмосферные оптические линии связи (на англ. – Free Space Optics) в своей архитектуре передачи и приема информации используют оптический инфракрасный сигнал в качестве канала связи с использованием оптических линз и систем для корректировки и автоматической наводки 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

Аппаратно-программные комплексы для передачи информации по атмосферным оптическим линиям связи имеют специальную конструкцию составных элементов для корректной передачи и отправки сигнала по инфракрасному оптическому сигналу. Структурная схема передачи информации по атмосферным оптическим линиям связи между аппаратно-программными комплексами имеет следующий вид (Рисунок 2):

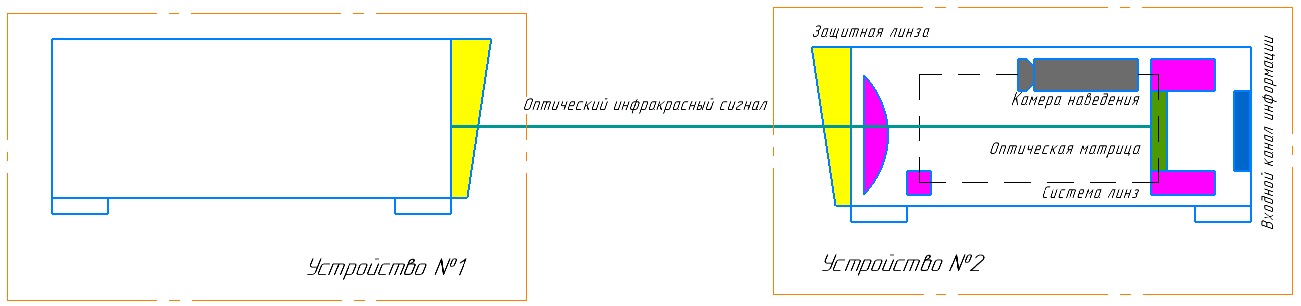


Рисунок 2 – Структурная схема устройства №1 (передатчик) и устройства №2 (приемник) для передачи и приема сообщения по атмосферным оптическим линиям связи

Аппаратно-программные комплексы, использующиеся для передачи и приема информации по атмосферным оптическим линиям связи в своей конструкции, имеют специализированные 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 в автоматическом режиме без использования аппаратного или программного обеспечения комплекса;
* камера наведения – самостоятельное устройство использующее в своем составе цифровую камеру и датчик расстояния необходимый для автоматического наведения передающего устройства в область видимости принимающего устройства для создания канала передачи данных большой разрядности;
* система линз – набор транспарентных и угловых линз образующих единую оптическую систему для компактного преобразования инфракрасного оптического сигнала внутри комплекса и передачи принятого сигнала с датчиков на оптическую матрицу;
* 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.

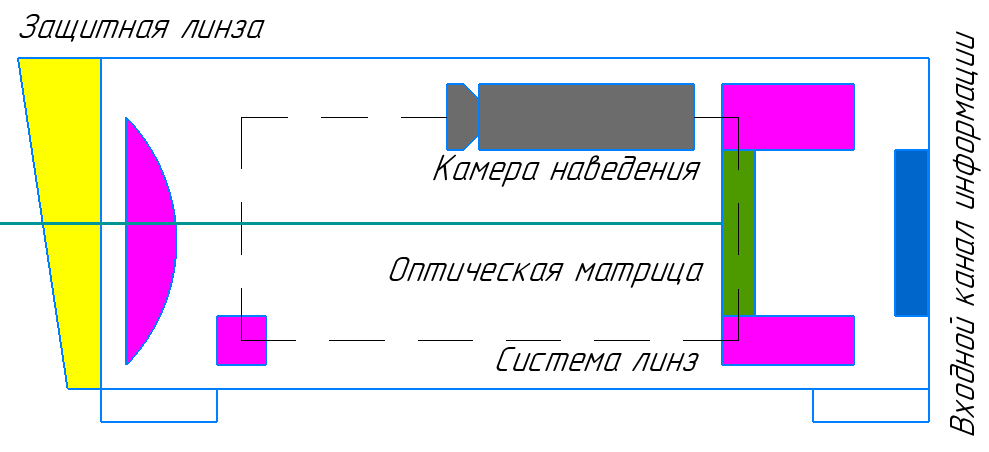


Рисунок 3 – Конструкция устройства для передачи и приема сообщения по атмосферным оптическим линиям связи

Инфракрасные лучи используемые в источниках генерации инфракрасного оптического сигнала имеют длину волны от 700 нм до 1 мм. При этом, в конструкции таких устройств обязательно используется система линз для корректировки, фокусировки и устранения эффектов оптической дифракции в процессе принятия и отправки информации. Инфракрасные лучи передают информацию в зоне прямой видимости приемника и передатчика без огибания препятствий в виде зданий, лесных массивов и других объектов которые могут служить в качестве препятствия для распространения инфракрасного оптического сигнала.

Во время передачи сигнала с помощью инфракрасного луча, используется сигнальная модуляция генерируемого сигнала, при этом модуляция изменяет сигнал, увеличивая или уменьшая его амплитуду и фазовую частоту в зависимости от массива данных поступаемых на входной канал информации. Для приема сигнала используется специальное устройство – фотодиод, суть которого заключается в преобразовании оптического сигнала в последовательность бинарного цифрового детерминированного сигнала на основе полупроводникового эффекта, при котором между частотой сигнала и напряжением на выходе формируется прямая пропорциональность для формирования логического сигнала в битовой последовательности.

Модуляция сигнала передаваемого с помощью инфракрасных лучей применяется для уплотнения сигнала и соответственно увелечения количества передаваемой информации по инфракрасному оптическому каналу связи. В зависимости от типа сигнала, применяются следующие типы модуляции (Рисунок 4):

* амплитудная модуляция является самым простым типом модуляцией сигнала с точки зрения аппаратной и программной реализации. Метод амплитудной модуляции заключается в изменении амплитуды сигнада для передачи информации и уплотнения информации передаваемой по инфракрасному оптическому каналу связи. В качестве достоинств можно отметить простотую реализации алгоритма амплитудной модуляции сигнала, относительную дешевизну оборудования и хорошее качестве модуляции низкочастотных сигналов. При этом, амплитудная модуляци не лишена недостатков, а именно – модуляция сигнала по амплитуде имеет низкую помехоустойчивость и эффективность использования канала данных, при этом уплотнение информации передаваемой по каналу данных, имеет прямую пропорциональность с дальностью распространения этого сигнала;
* частотная модуляция изменяет сигнла с помощью изменения частоты и настройки тактирования передаваемого сигнала с помощью цифровых устройств и высокоскоростных протоколов передачи информации. Достоинства частотной модуляции заключаеются в хорошем качестве передаваемого сигнала при высокой помехоустойчивости канала данных вкупе с эффективным использованием канала передачи данных. При этом, частотная модуляция не всегда достигается эффективным способом из-за необходимости интегрированя сигнала по частоте. Кроме этого, оборудование использующее частотную модуляцию имеет большую сложность в разработке, проектирования и обслуживании;
* импульсно-кодовая модуляция изменяет сигнал с помощью создания последовательности импульсов для передачи информации и внедрения кодовой информации в передаваемый сигнал. Импульсно-кодовая модуляция применяется в устройствах, где имеется ограничение по ширине канала данных, ввиду того что импульсно-кодовая модуляция имеет высокую скорость передачи данных и помехоустойчивость, при этом сложность реализации такого принципа модуляция ложится на инженеров аппаратного обеспечения ввиду необходимости использования высокочастотных элементов.

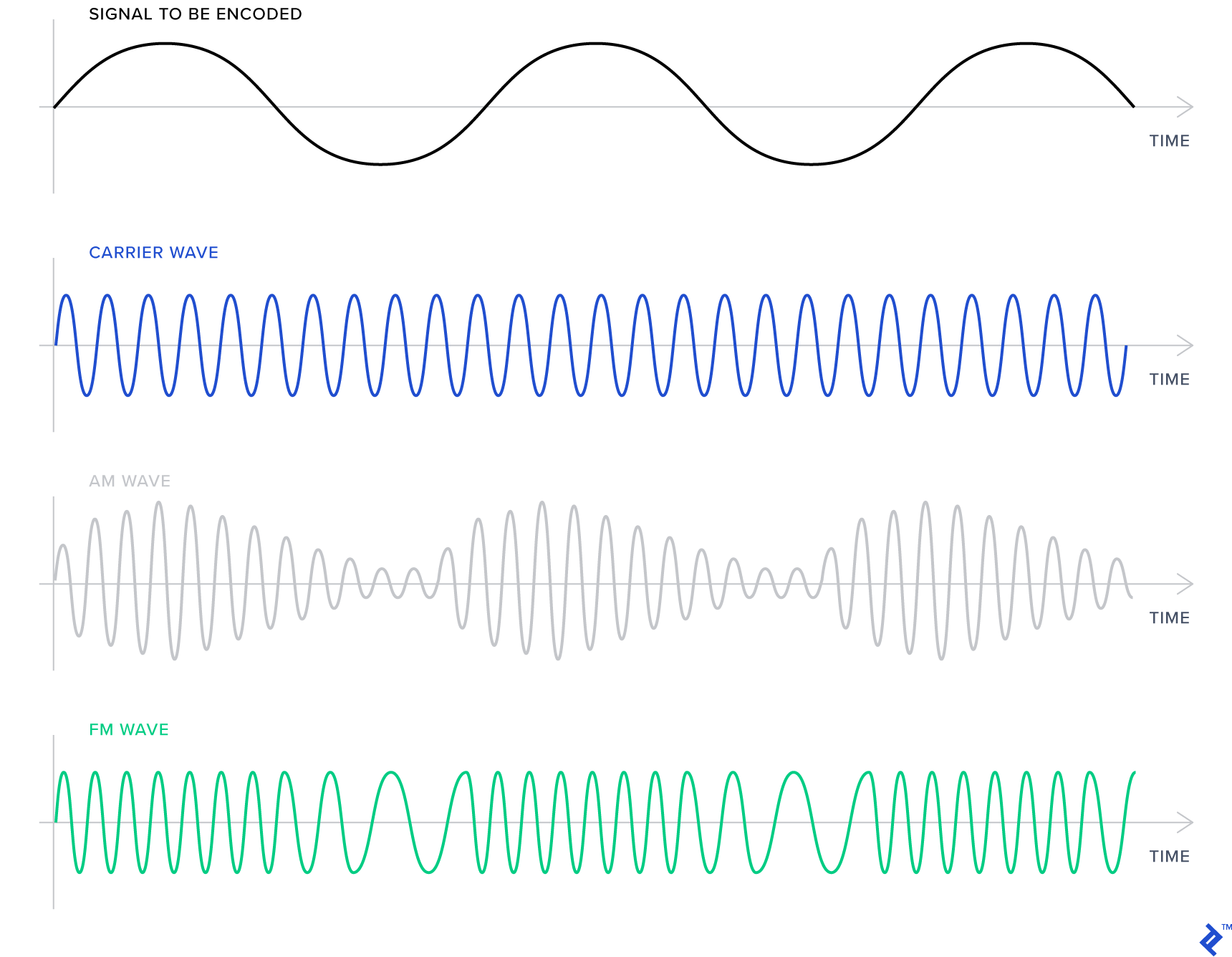


Рисунок 4 – Изменение сигнала с помощью различных типов модуляции

## Описание целей разработки

Цель разработки комплекса для безопасной передачи сообщения по инфракрасному оптическому каналу связи заключается в проектировании аппаратно-программного комплекса, главной задачей которого является передача и прием информации по инфракрасному каналу связи с предварительным шифрованием.

Для обеспечения надежной передачи информации по инфракрасному оптическому каналу связи необходимо обеспечить нужный уровень защиты передаваемой информации с помощью предварительно настроенных алгоритмов шифрования, оптимизированных для использования с микроконтроллерной платформой обладающей низкой производительностью по сравнению с персональными и одноплатными компьютерами (Рисунок 5).

Рисунок 5 – Цели разработки комплекса

Для передачи и приема инфракрасного оптического сигнала используются инфракрасный диод, генерирующий волну с определенной частотой, амплитудой и импульсом и передающий зашифрованную информацию в виде инфракрасного сигнала в сторону устройства-приемника, где расположен фотодиод в качестве принимающего оптического сенсора.

## 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

Системы автоматизированного проектирования, интегрированные среды разработки программного обеспечения, а также аппаратные средства обеспечения комплекса можно разделить на четыре основные группы:

* аппаратное обеспечение;
* программное обеспечение комплексные системы управления содержимым, предполагающие определенный набор инструментов для работы с веб-контентом;
* криптографя;
* 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 большую. 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 2022* (см. Рисунок 3).
2. Среда анализа и моделирования печатной платы – *Cadence Sigrity 2022* (см. Рисунок 4).

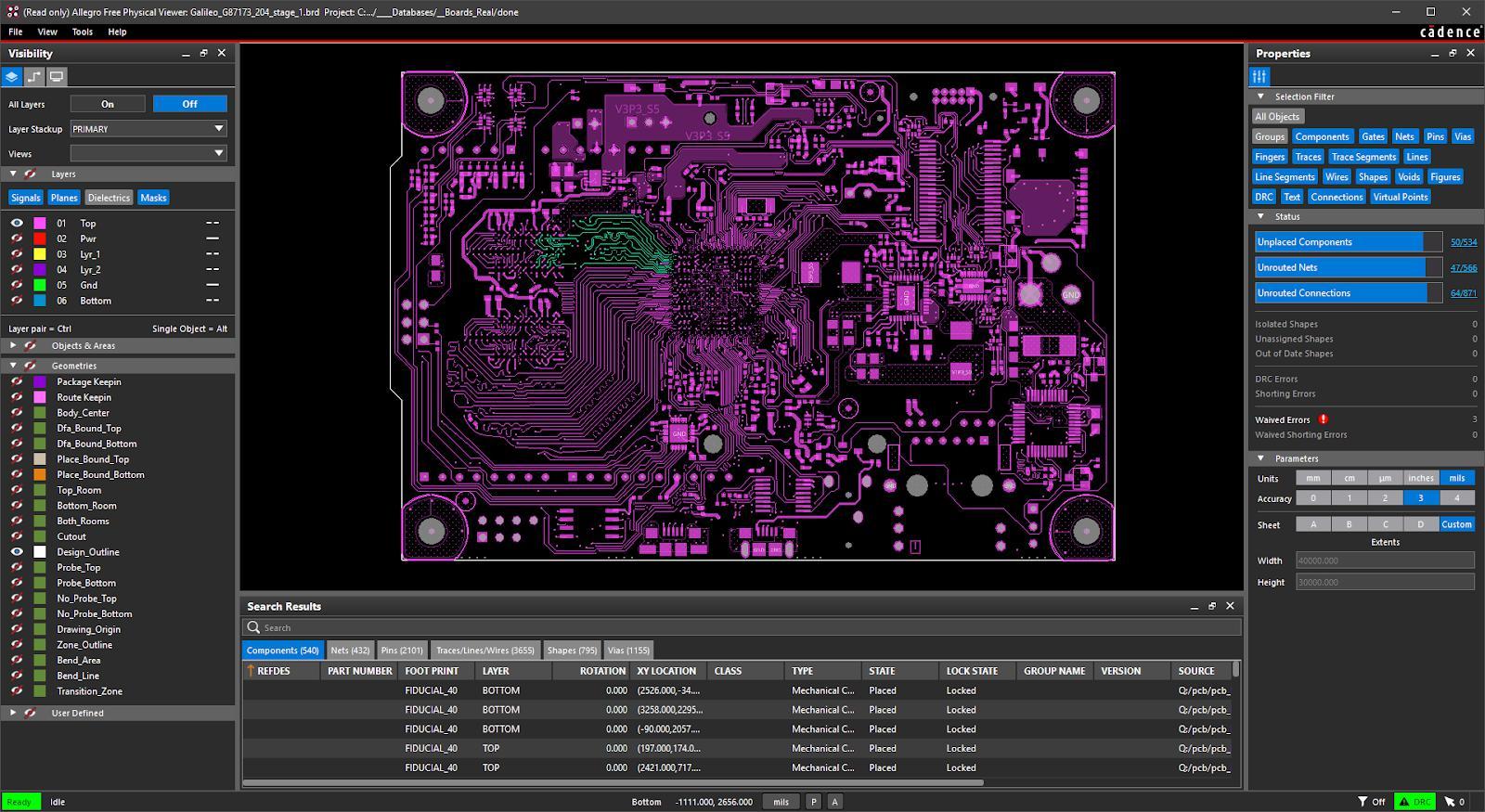


Рисунок 3 – Внешний вид Cadence Allegro PCB Designer 17.4

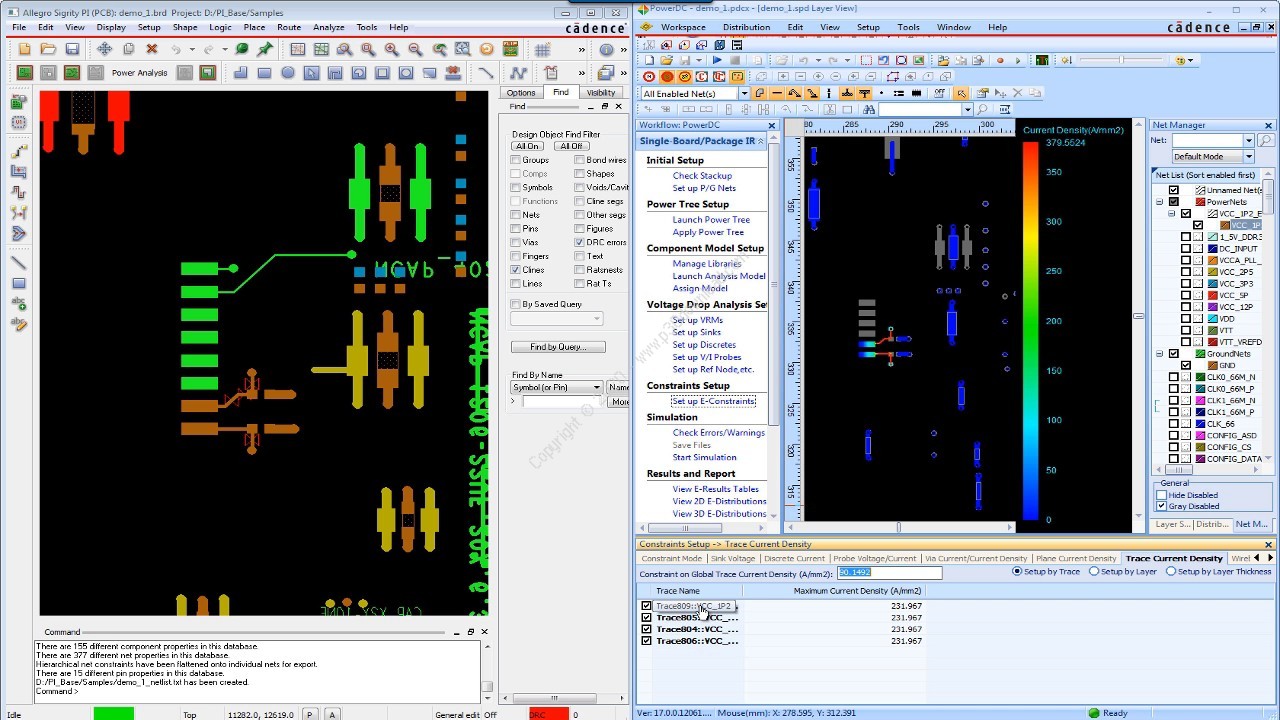


Рисунок 4 – Внешний вид Cadence Sigrity 2019

*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).

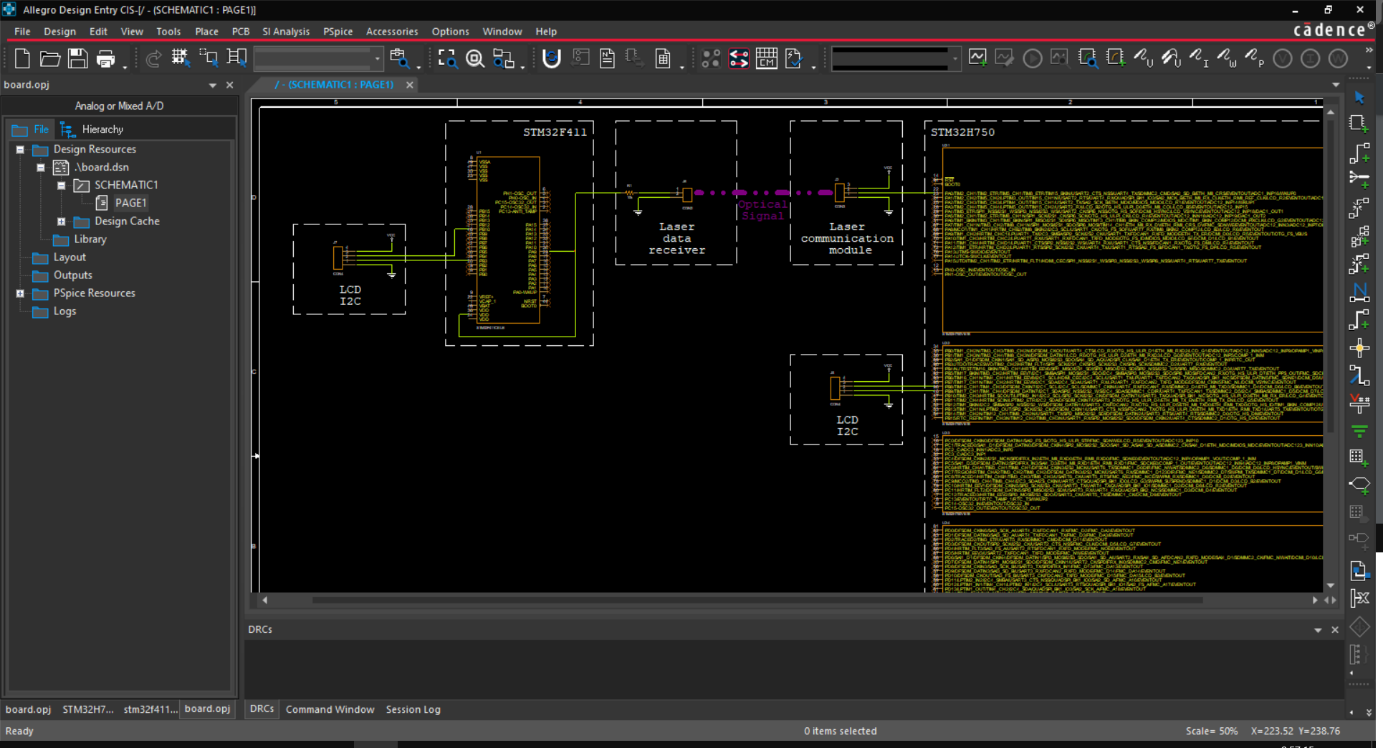


Рисунок 5 – Электрическая схема устройства спроектированная в Cadence Allegro Design CIS

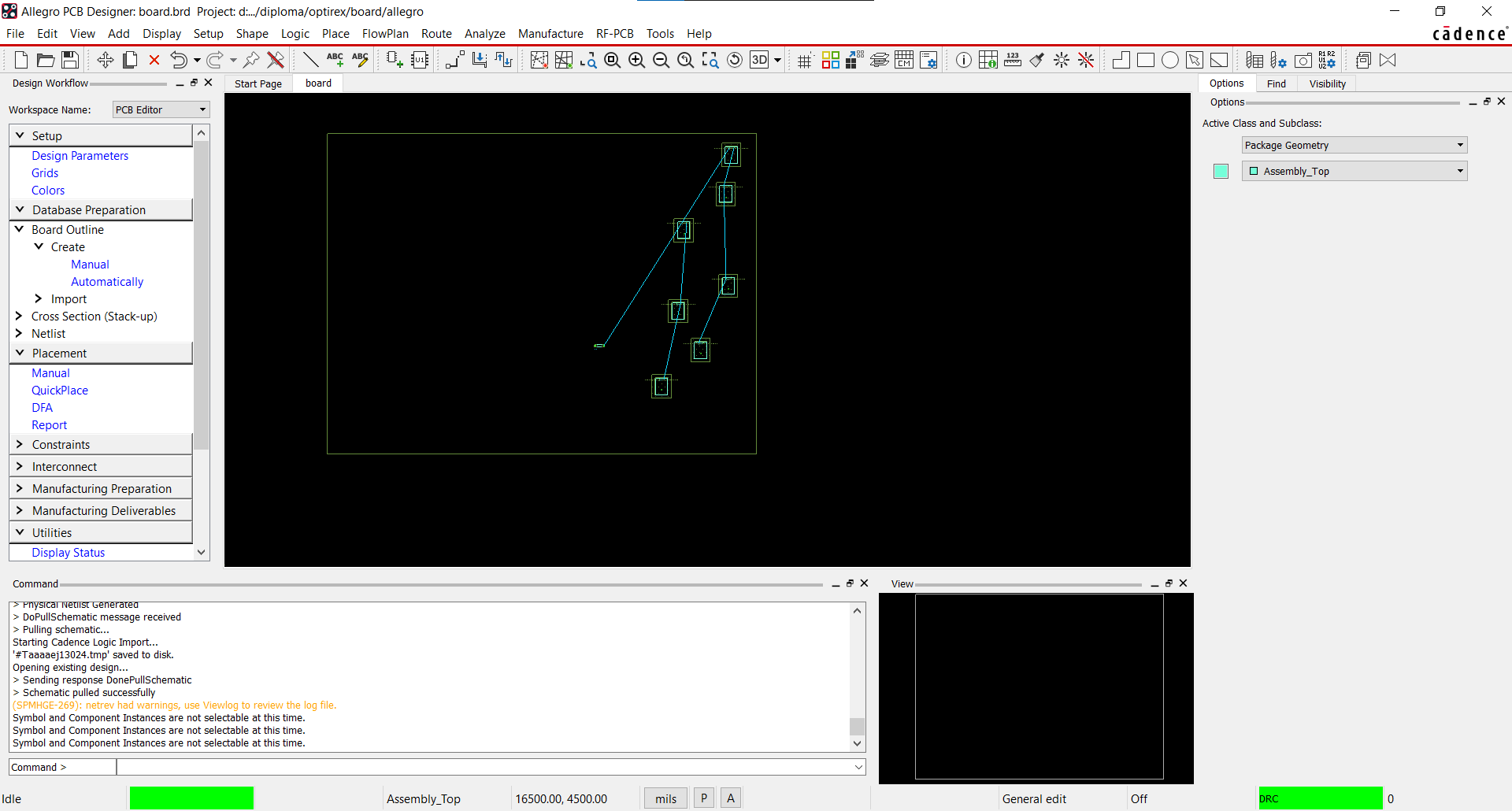
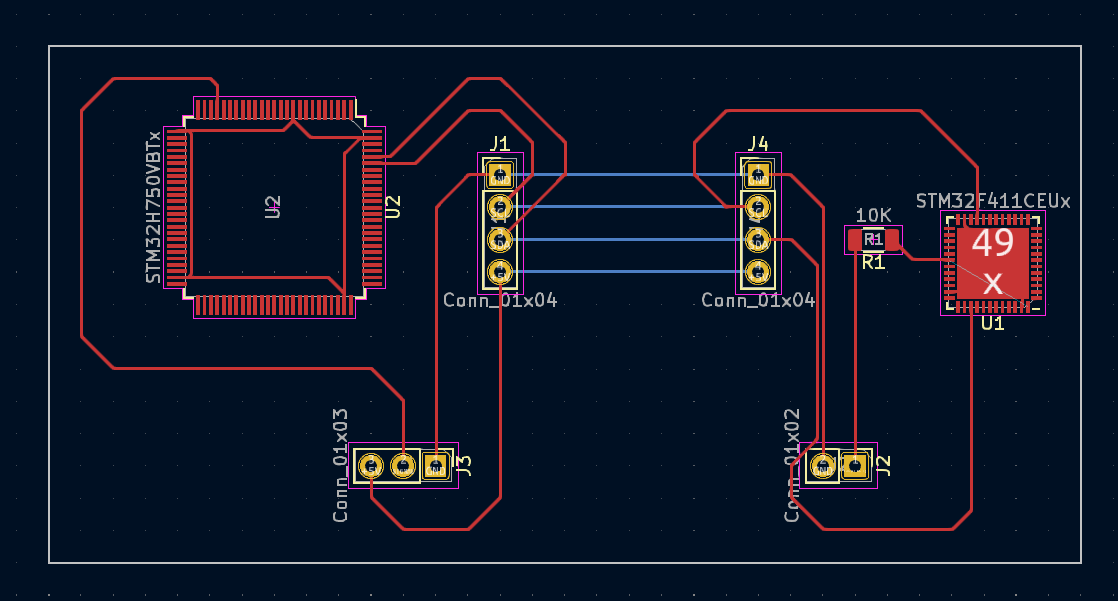


Рисунок 6 – Печатная плата на основе созданной электрической схемы Cadence Allegro PCB Designer

*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.

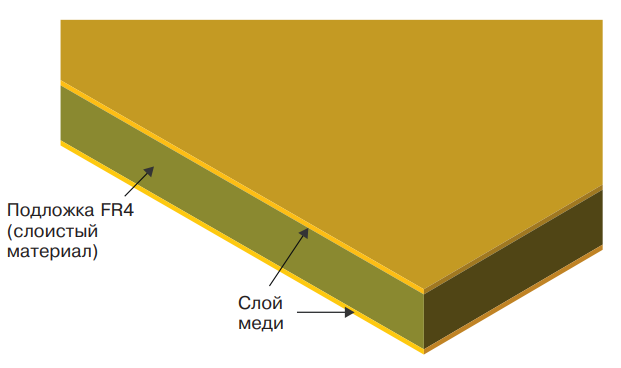
****

Рисунок 1 – Топология двухслойной печатной платы

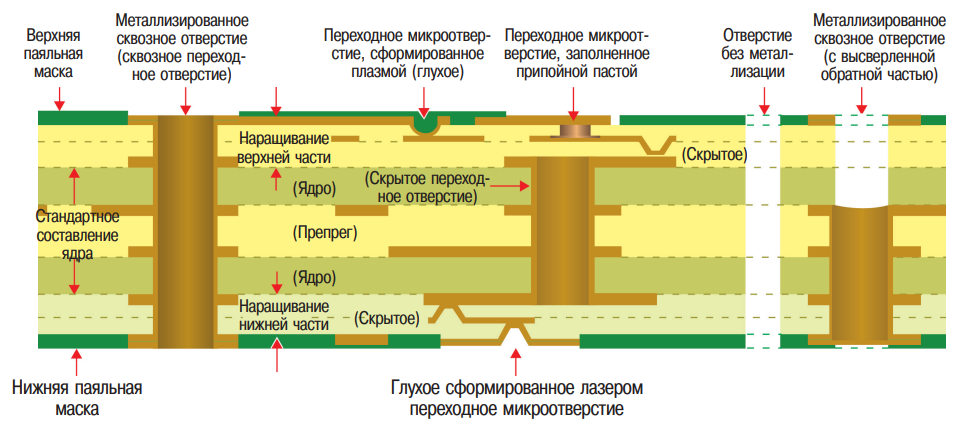
****

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].

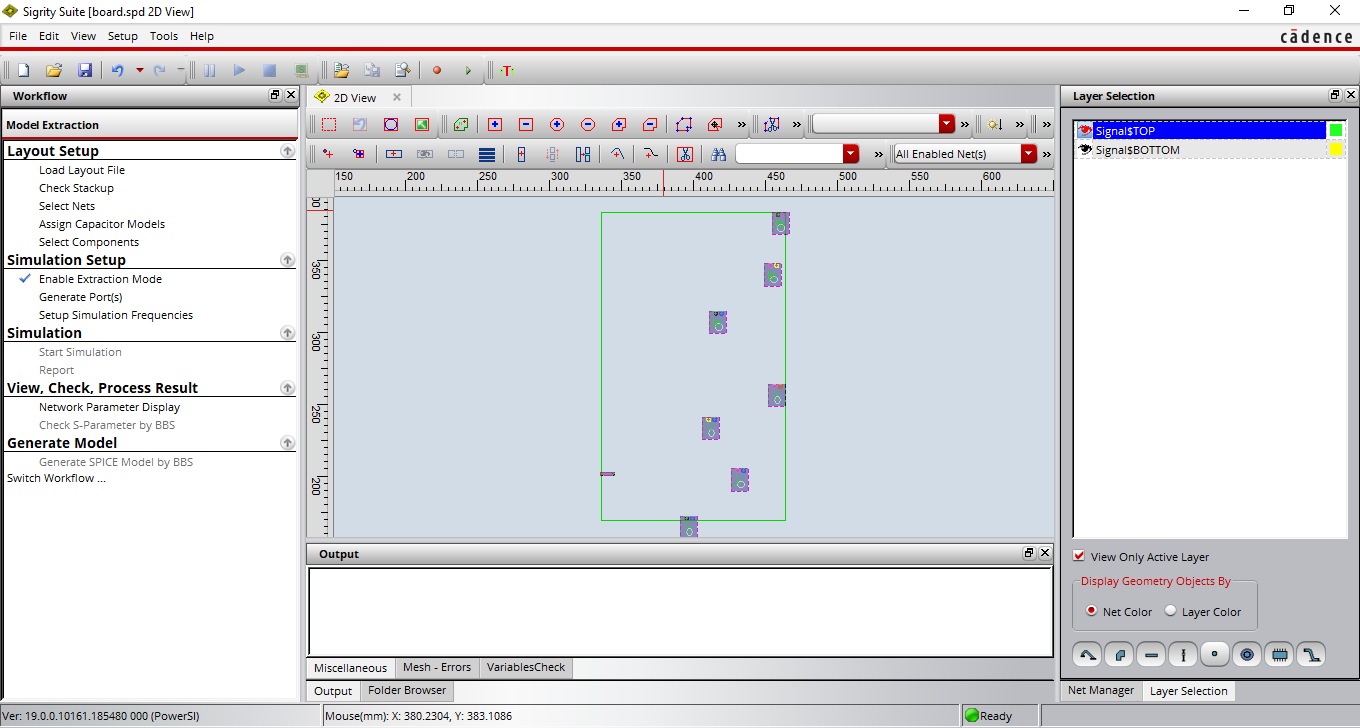


Рисунок 7 – Анализ печатной платы в Cadence Sigrity 2019 PowerSI

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).

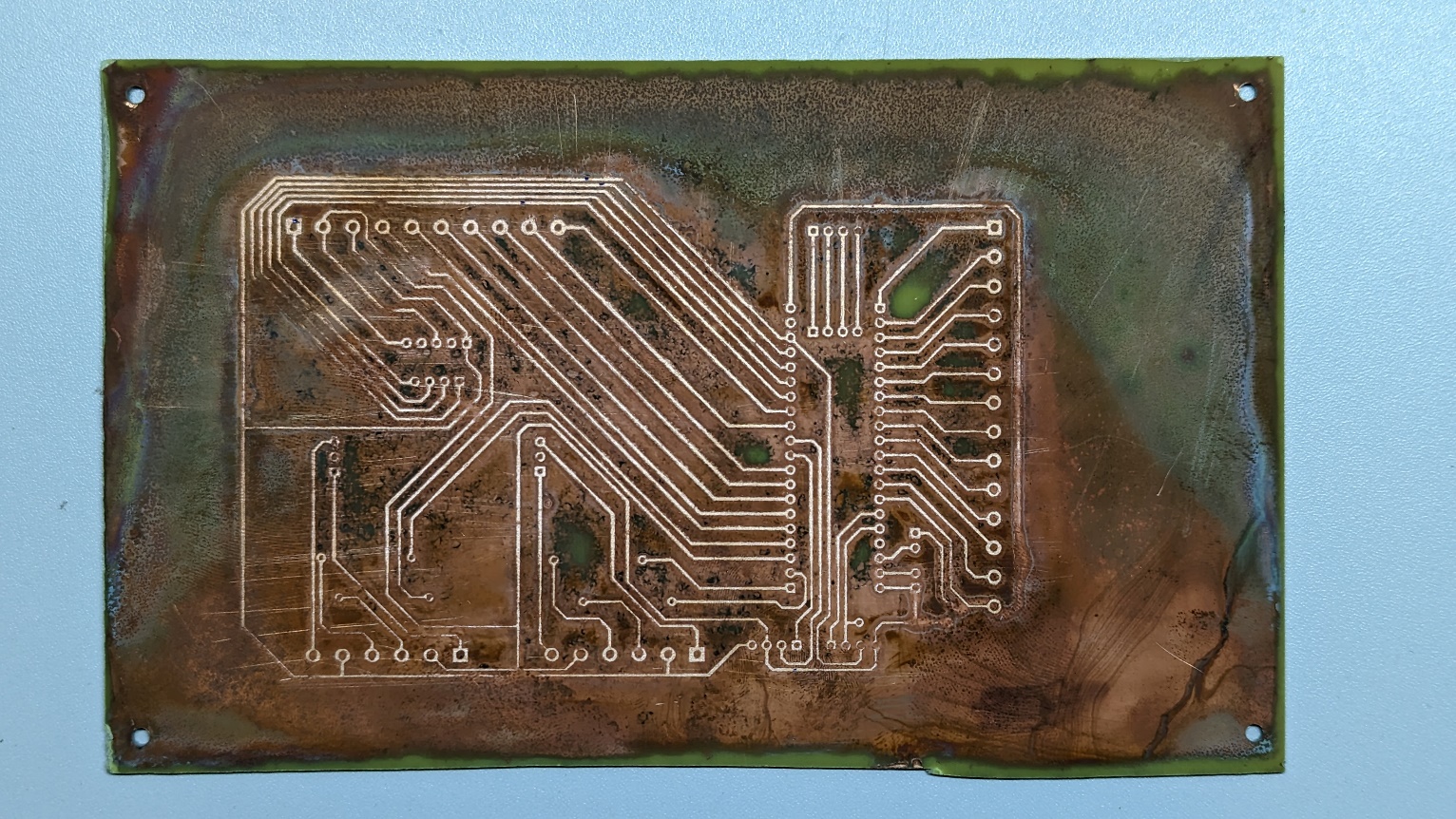


Рисунок 10 – Первая версия печатной платы устройства

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.

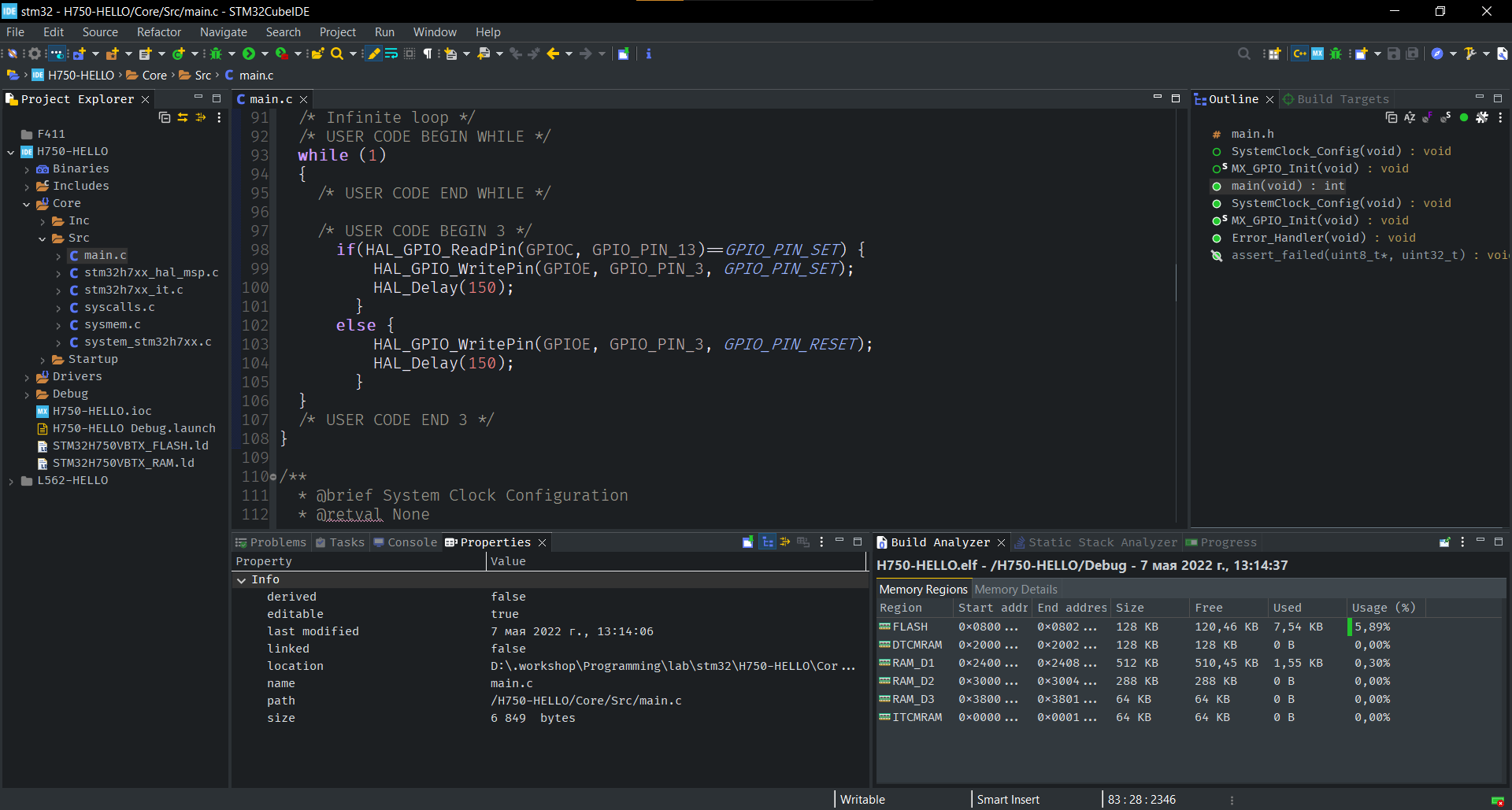


Рисунок 12 – Разработка и отладка программного кода встраиваемых систем на основе микроконтроллера ARM промышленного стандарта с использованием IDE STM32CubeIDE

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

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.

Победителем конкурса в 1998 году стал алгоритма «Rijndael», названный по инициалам его авторов – бельгийскими криптографами Джоаном Даменом и Винсентом Рейменом. При разработке криптографического алгоритма AES разработчики предусмотрели все слабые места алгоритма DES, а также его усовершенствованных вариаций и алгоритмов на основе сетей Фейстеля – TDES, Blowfish, DEA.

Криптографический алгоритм AES является блочным шифром с раундовым шифрованием информации с переменной длиной ключа и фиксированными длинами входного и выходного блоков шифрования. Длина ключа зависит от применения криптографического алгоритма – вычислительные системы с малой степенью интеграции и производительности имеют длину ключа в 128 бит, и напротив – вычислительные системы с высоким уровнем производительности имеют длину ключа в 192 либо 256 бит. Фиксированная длина входного и выходного блоков шифрования имеет длину в 128 бит для упрощения аппаратной и программной имплементации криптографического алгоритма на разных вычислительных системах в независимости от цифровой архитектуры центрального процессора или операционной системы.

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 инфракрасных оптических систем в сфере телекоммуникаций специального и общего назначения не оспаривается ввиду наличия преимуществ по сравнению с другими типами передачи информации. Предприятия, объекты и организации, имеющие критическую информационную инфраструктуру, увеличиваются инвестиции, направленные на развитие защищенных телекоммуникационных систем специального и общего назначения для передачи зашифрованной информации.

Разработанный аппаратно-программный комплекс для безопасной передачи сообщения по оптическому каналу связи повышает защищенность телекоммуникационных систем специального назначения за счет использования аппаратно-программных криптографических алгоритмов, повышающих скорость потокового шифрования информации и уровня защищенности передаваемой информации с помощью инфракрасного оптического сигнала.

В ходе выполнения выпускной квалификационной работы был разработан аппаратно-программный стенд для безопасной передачи сообщения по инфракрасному оптическому каналу связи между двумя устройствами – приемником и передатчиком с использованием оптимизированных криптографических алгоритмов для аппаратно-программного ускорения потокового шифрования информации.

В данной работе была спроектирована, указана и продемонстрирована чертежно-конструкторская документация на разработанные устройства для безопасной передачи сообщения по инфракрасному оптическому каналу связи, а также программное обеспечение необходимое для потокового шифрования передающейся информации оптимизированного для микроконтроллерной платформы общего назначения.

Целью в данной выпускной квалификационной работе было создание аппаратно-программного комплекса для безопасной передачи информации по оптическому каналу связи и применение данного комплекса в обучении студентов учреждений технического и профессионального образования по специальностям и квалификациям, связанным с аппаратно-программными комплексами информационной безопасности и основам сигнальной передачи в высокоскоростной электронике.

Для реализации данного проекта был выбран язык C++, а в качестве аппаратной платформы – микроконтроллеры STM32 семейства H7. Для создания аппаратного и программного обеспечения комплекса были выбраны следующие системы автоматизированного проектирования:

* Cadence Allegro 2022 – для проектирования электрических схем и трассировки электронных компонентов и печатных плат;
* Cadence Sigrity 2022 – для системного анализа печатных плат по тепловым, сигнальным и физическим характеристикам;
* STM32CubeIDE – для проектирования программного обеспечения и оптимизации криптографических алгоритмов;

Цель выпускной квалификационной работы достигнута – разработан аппаратно-программный комплекс для безопасной передачи сообщения по оптическому каналу связи с использованием оптимизированных криптографических алгоритмов. Архитектура комплекса прошла все физические, аппаратные и программные тесты для соответствия всем заявленным характеристикам.

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.

Разработка аппаратно-программного комплекса для безопасной передачи сообщения по оптическому каналу связи позволяет дополнительно изучить аспекты проектирования высокоскоростной электроники и печатных плат, программирования встраиваемых систем на основе промышленных микроконтроллеров, основ передачи зашифрованной информации с помощью оптических систем и использование оптимизированных криптографических алгоритмов для микроконтроллерных платформ общего назначения.

# СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Thaker N.B., Ashok R., Manikandan S., Nambath N., Gupta S., – «A Cost-Effective Solution for Testing High-Performance Integrated Circuits»; IEEE TRANSACTIONS ON COMPONENTS PACKAGING AND MANUFACTURING TECHNOLOGY, 2021. – 7 p.
2. Yi Z.C., Feng H.Q., Zhou X.F., Shui L.L., – "Design of an Open Electrowetting on Dielectric Device Based on Printed Circuit Board by Using a Parafilm M"; FRONTIERS IN PHYSICS, 2020. – 8 p.
3. Zhang Y., Liu Z.Y., Zhang X.L., Guo S.Y., – "Sandwich-Layered Dielectric Film with Intrinsically Excellent Adhesion, Low Dielectric Constant, and Ultralow Dielectric Loss for a High-Frequency Flexible Printed Circuit"; INDUSTRIAL & ENGINEERING CHEMISTRY RESEARCH, 2021. – 10 p.
4. Park H., Song J., Sim J., Choi Y., Choi J., Yoo J., Kim C., – "30-Gb/s 1.11-pJ/bit Single-Ended PAM-3 Transceiver for High-Speed Memory Links"; IEEE JOURNAL OF SOLID-STATE PHYSICS, 2021. – 9 p.
5. Pace L., Idir N., Duquesne T., De Jaeger J.C., – "Parasitic Loop Inductances Reduction in the PCB Layout in GaN-Based Power Converters Using S-Parameters and EM Simulations"; ENERGIES, 2021. – 15 p.
6. Mitzner K., «Complete PCB Design Using OrCAD Capture and PCB Editor» – Second Edition. – Elseiver Academic Press, 2019. – 600 p.
7. 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.
8. Труднов А.В., «Высокоскоростные печатные платы. Записки схемотехника», – Москва: Ridero, 2020. – 108 с.
9. Труднов А.В., «Высокоскоростные печатные платы. Теоретические рекомендации», – Москва: Ridero, 2019. – 156 с.
10. Труднов А.В., «Высокоскоростные печатные платы. Практические рекомендации», – Москва: Ridero, 2019. – 152 с.
11. Кечиев Л.Н., «Печатные платы и узли гигабитной электроники», – Москва: Библиотека ЭМС, 2017. – 424 с.
12. Ardizoni J., «Practical guide to design high-speed printed circuit boards» – Cadence Publisher, 2019. – 20 p.
13. Bogatin E., «Practical guide to transmission line design and characterization for signal integrity applications» – Artech House, 2020. – 604 p.
14. Griffin B., «Cadence Sigrity 2019 Release Function» – Cadence Publisher, 2019. – 56 p.
15. Коберниченко В.Г., «Основы цифровой обработки сигналов», – Изд-во Урал. Ун-та, 2018. – 150 с.
16. Белоус А.И., Солодуха В.А., Шведов С.В., «Основы конструирования высокоскоротных электронных устройство», –Москва: Техносфера, 2017. – 872 с.
17. Пош М., «Программирование встроенных систем на C++ 17» / пер. с англ. А.В. Снастина. – М.: ДМК Пресс, 2020. – 394 с.
18. Альфред, В. Ахо., «Компиляторы. Принципы, технологии и инструментарий» / Альфред В. Ахо и др. – Москва: Высшая школа, 2015. – 882 c.
19. Ашарина И.В., «Основы программирования на языках С и С++: Курс лекций для высших учебных заведений» / И.В. Ашарина. — М.: Гор. линия-Телеком, 2018. — 208 c.
20. Герберт, Шилдт «C++. Базовый курс» / Шилдт Герберт. – М.: Диалектика / Вильямс, 2022. – 564 c.
21. Дейтел, Пол «Как программировать на С» / Пол Дейтел , Харви Дейтел. – М.: Бином, 2022. – 858 c.
22. Владимиров С.М., Габидулин Э.М., Колыбельников А.И., Кшевецкий А.С., «Криптографические методы защиты информации.» – М.: Издательство Московского Государственного Университета, 2021. – 433 с.
23. Беляков С.Л., Боженюк А.В., Петряева М.В., «Основы разработки программы на языке C++ для систем информационной безопасности: учебное пособие». – М.: Издательство Южного Федерального Университета, Ростов-на-Дону, 2020. – 152 с.
24. Novello K., «Mastering STM32». – М.: Leanpub Publishing, 2022. – 910 p.
25. AN5156 Application Note – Introduction to STM32 microcontrollers security., 2019. – 55 с.