

**Факультет «Информационные технологии»**

**ОТЧЕТ**

**по прохождению преддипломной практики**

|  |  |  |
| --- | --- | --- |
| **Выполнил**  **студент, группа** | И-19-2Р  (группа) | Мольганов А.А.  (Ф.И.О., роспись) |
|  |  |  |
|  |  |  |
| **Научный**  **руководитель**  **от предприятия** | Руководитель ОП  (должность) | Вафаев А.Р.  (Ф.И.О., роспись) |
|  |  |  |
|  |  |  |
| **Научный**  **руководитель**  **от университета** | Проректор по АиНД, ассоц.профессор, PhD  (должность) | Савельева В.В.  (Ф.И.О., роспись) |

**АЛМАТЫ 2023 г.**

**Содержание**

|  |  |
| --- | --- |
| Введение | **2** |
| Общая характеристика ТОО «НПО «Группа Компаний «DOSTI» | **4** |
| Должностные обязанности | **5** |
|  |  |
| **Глава 1.** Аппаратное обеспечение комплекса |  |
| 1.1. Проектирование высокоскоростных печатных плат | **6** |
| 1.2. Моделирование реальных условий работы высокоскоростной печатной платы | **12** |
| 1.3. Исправление неисправностей, возникших при проектировании печатной платы | **14** |
|  |  |
| **Глава 2.** Программное обеспечение комплекса |  |
| 2.1. Программное окружение для создания встраиваемых приложений | **15** |
| 2.2. Оптимизация встраиваемых приложений с учетом возможностей микроконтроллера | **20** |
|  |  |
| **Глава 3.** Разработка криптографического алгоритма и адаптация алгоритма под аппаратно-программные требования комплекса |  |
| 3.1. Криптографический алгоритм AES-256 | **22** |
| 3.2. Оптимизация алгоритма AES-256 | **23** |
| 3.3. Использование аппаратных средств защиты информации | **25** |
|  |  |
| Заключение | **28** |
| Список использованных источников | **30** |

**Введение**

Преддипломная практика является завершающим этапом образовательного процесса, главной целью которого является подготовка и выпуск высококвалифицированного кадра на рынок труда. Материально-техническое и информационное обеспечение преддипломной практики прежде всего зависит от места прохождения и специализации студента.

Основное содержание преддипломной практики на протяжении 12 недель заключается в выполнении практических, творческих и исследовательских проектов, соответствующих характеру, профилю и специализации будущей профессиональной деятельности студента с учетом оснащения места прохождения практики.

*Цели преддипломной практики:*

1. Закрепление теоретических знаний, полученных во время образовательного процесса.
2. Проведение экспериментальных, исследовательских и практических проектов в соответствии с профилем и специализации студента и образовательной программы.
3. Сбор информации и материалов для выполнения выпускной квалификационной работы согласно установленным требованиям.

*Задачи преддипломной практики;*

1. Закрепление полученных теоретических знаний во время образовательного процесса.
2. Получение первоначального опыта работы с оборудованием, материалами и другими изделиями в реальных условиях на производстве.
3. Сбор информации и материалов для успешного выполнения выпускной квалификационной работы согласно установленным требованиям;
4. Формирование системного мышления и профессиональной позиции студента, мировоззрения, стиля поведения и освоение профессиональной этики.
5. Приобретение навыков корпоративной, индивидуальной, командной и совместной работы в профессиональных группах, члены которой обладают различными специальностями, должностями и званиями.

*Процесс прохождения преддипломной практики направлен на формирование следующих компетенций:*

1. Навыки использования нормативно-правовых документов в профессиональной деятельности.
2. Стремление к саморазвитию, повышению квалификации и мастерства.
3. Умение критически оценивать достоинства и недостатки, исследовать пути и выбрать средства самосовершенствования.
4. Осознание социальной значимости своей будущей профессии, обладает высокой мотивацией к выполнению профессиональной деятельности.
5. Способность анализировать и определять требования к проекту различной сложности.
6. Способность составлять подробную спецификацию требований к проекту различной сложности.
7. Способность синтезировать набор возможных решений задачи или подходов к выполнению проектов различной сложности.
8. Способность научно и аргументированно обосновать свои предложения, идеи и мысли.

**Общая характеристика ТОО «НПО «Группа Компаний «DOSTI»**

Инновационный центр «DOSTI» предоставляет широкий спектр направлений в сфере робототехники, электроники и мехатроники для обучения и индивидуального развития. Компания является официальным партнером и спонсором движения WorldSkills Kazakhstan, которое направлено на поднятие престижа и развития рабочих специальностей в учреждениях средне-специального и высшего образования Республики Казахстан.

Также совместно с НАО "Talap" при поддержке Министерства Образования и Науки Республики Казахстан, компания активно участвует в разработке современных инновационных программ обучения по различным компетенциями согласно программе международных чемпионатов WorldSkills International в учреждениях средне-специального и высшего образования Республики Казахстан.

*Направления, которые охватывает компания:*

1. Проектирование, разработка и выпуск электротехнических устройств и изделий.
2. Проектирование, разработка и выпуск прикладного программного обеспечения.
3. Проектирование, разработка и выпуск мехатронных и робототехнических систем стационарного и мобильного назначения.
4. Проектирование, разработка и выпуск твердотельных изделий на основе аддитивных технологий.

Компания имеет в своей структуре 2 ключевых отдела отвечающих за деятельность компании:

1. *Учебно-методический отдел.* Данный отдел ответственен за организацию и проведение курсов обучения, повышения квалификации, подготовки к чемпионатам WorldSkills Kazakhstan и International, за написание учебных пособий, методических указаний, учебных планов и программ, за проведение учебных и производственных практик для студентов колледжей и университетов. Отдел отвечает за создание новых продуктов (проектов, устройств и т.п.), анализ и подготовку материалов для продуктов, подлежащих промышленному производству.
2. *Проектно-производственный отдел.* Данный отдел ответственен за производство продуктов (электротехнических устройств и изделий) компании. Отдел имеет в своем распоряжении лабораторию, укомплектованную всем необходимым оборудованием для производства электронных устройств начиная от печатных плат и заканчивая корпусами устройств. Проектно-производственный отдел принимает студентов на практику в ограниченном количестве после прохождения комплексного тестирования определяющих индивидуальные навыки и умения каждого практиканта.

**Занимаемая должность на производстве**

1. **Название должности**: Инженер-разработчик;
2. **Специализация должности**: Инженер-разработчик встраиваемых систем;
3. **Уровень должности**: Начальный (Junior);
4. **Опыт работы**: не менее 3 месяцев;
5. **Описание должности**:

Инновационный центр «DOSTI» предоставляет широкий спектр направлений в сфере робототехники, электроники и мехатроники для обучения и индивидуального развития. Разработка учебных стендов и продуктов аппаратно-программного обеспечения является основной производственной формой компании.

Инженер-разработчик встраиваемых систем отвечает за комплексную интеграцию аппаратного и программного комплекса встраиваемой системы и оформление первоначальной чертежно-конструкторской документации на разрабатываемое устройство (встраиваемую систему).

1. **Должностные обязанности**:
   1. Участие в концептуальной и структурированной разработке встраиваемых систем широкого назначения.
   2. Разработка необходимого программного обеспечения для проведения отладочных, тестовых и пусконаладочных работ в сфере комплексного проектирования встраиваемых систем.
   3. Разработка электрической принципиальной схемы встраиваемой системы и согласование этапов разработки с командой.
   4. Разработка печатной платы на основе спроектированной электрической принципиальной схемы разрабатываемой встраиваемой системы и согласование этапов разработки с командой.
   5. Анализ, моделирование и исправление конструктивных недостатков, выявленных в процессе производства опытно-промышленной и мелкосерийной партии устройств.
2. **Требования к занимаемой должности**:
   1. Практический опыт в области электроники и полупроводниковой физики.
   2. Навыки владения персональным компьютером и прикладными программами в совершенстве.
   3. Практический опыт разработки в области моделирования электроники при помощи системы автоматизированного проектирования и прикладных программных пакетов анализа и моделирования.
   4. Практический опыт разработки в области написания программного кода для микроконтроллеров и микропроцессоров на языках программирования C и C++.

**Глава 1. Аппаратное обеспечение комплекса**

**1.1. Проектирование высокоскоростных печатных плат**

Современное развитие информационно-коммуникационных технологий требует постоянного совершенствования информационных систем и комплексов обработки данных. Развитие информационных систем, их суть, задачи и роль сводится к автоматизации различных бизнес-процессов. Информационная система имеет заранее определенную топологию в зависимости от задач, и требует от инженера-разработчика определенных навыков в области проектирования, разработки и пусконаладки информационных систем.

Информационная система имеет в своем составе следующую топологию:

1. *Аппаратное обеспечение* – включает в себя физические устройства, серверы, мейнфреймы, периферийные устройства, центры обработки данных.
2. *Программное обеспечение* – включает в себя операционные системы, системное и прикладное программное обеспечение, систему управления базами данных, программное обеспечение для обработки данных.
3. *Телекоммуникационное обеспечение* – включает в себя средства телекоммуникационной связи и передачи данных.
4. *Обеспечение безопасности* – включает в себя средства обеспечения безопасности информационной системы от несанкционированного доступа.

Увеличение массивов обработки данных с появлением глобальной сети Интернет, потребовало от инженеров-разработчиков аппаратного обеспечения использовать методы, средства и протоколы высокоскоростного обмена информации между составными компонентами, расположенными на печатной плате компьютера [1].

*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, эхо-локаторы и различные телекоммуникационные комплексы.

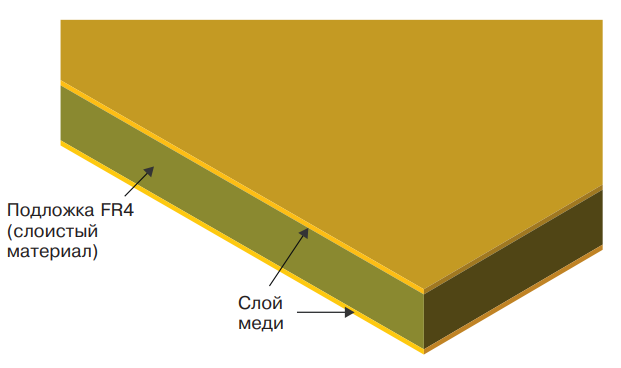
****

Рисунок 1 – Топология двухслойной печатной платы

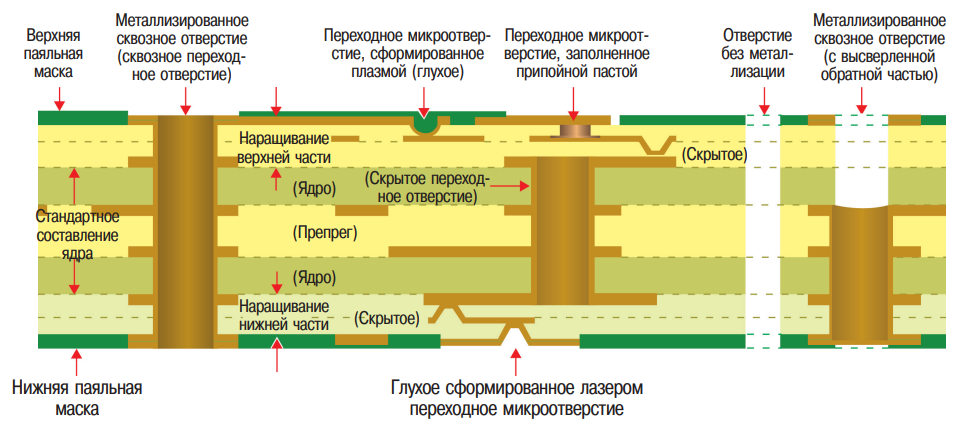
****

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.

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

Системы автоматизированного проектирования для электроники классифицируются по функционалу, стоимости и наличию среды моделирования (см. 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 прохождение преддипломной практики и выполнение всех практических заданий происходило 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).

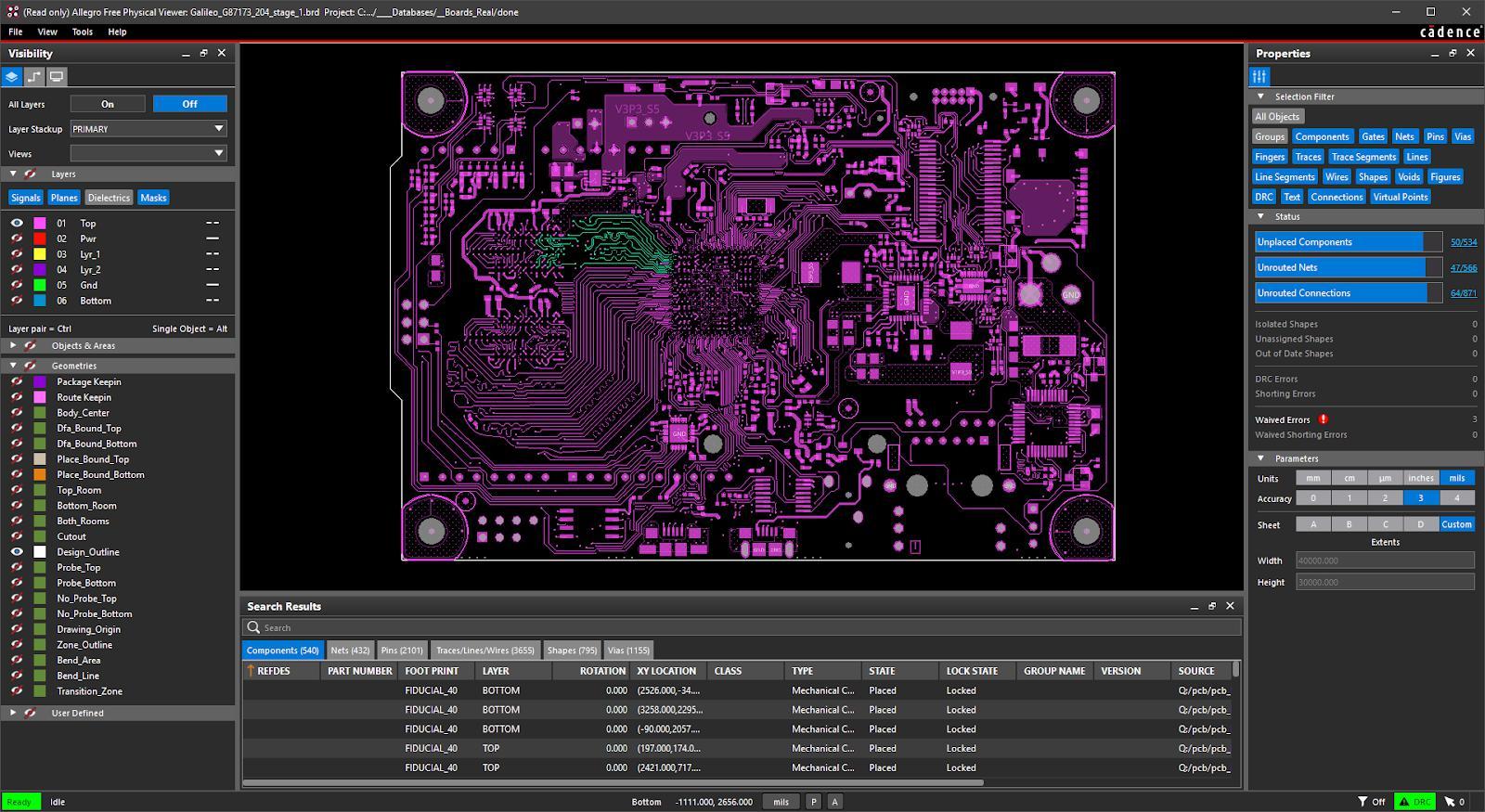


Рисунок 3 – Внешний вид Cadence Allegro PCB Designer 17.4

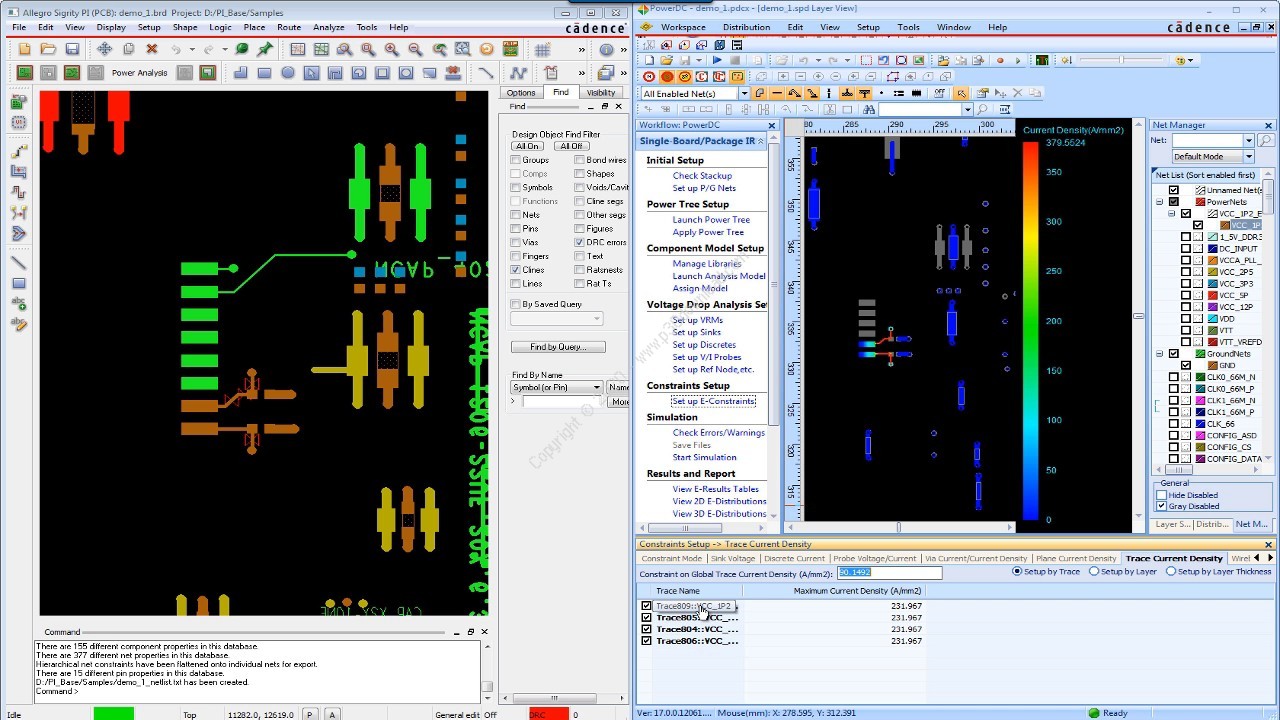


Рисунок 4 – Внешний вид Cadence Sigrity 2019

*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).

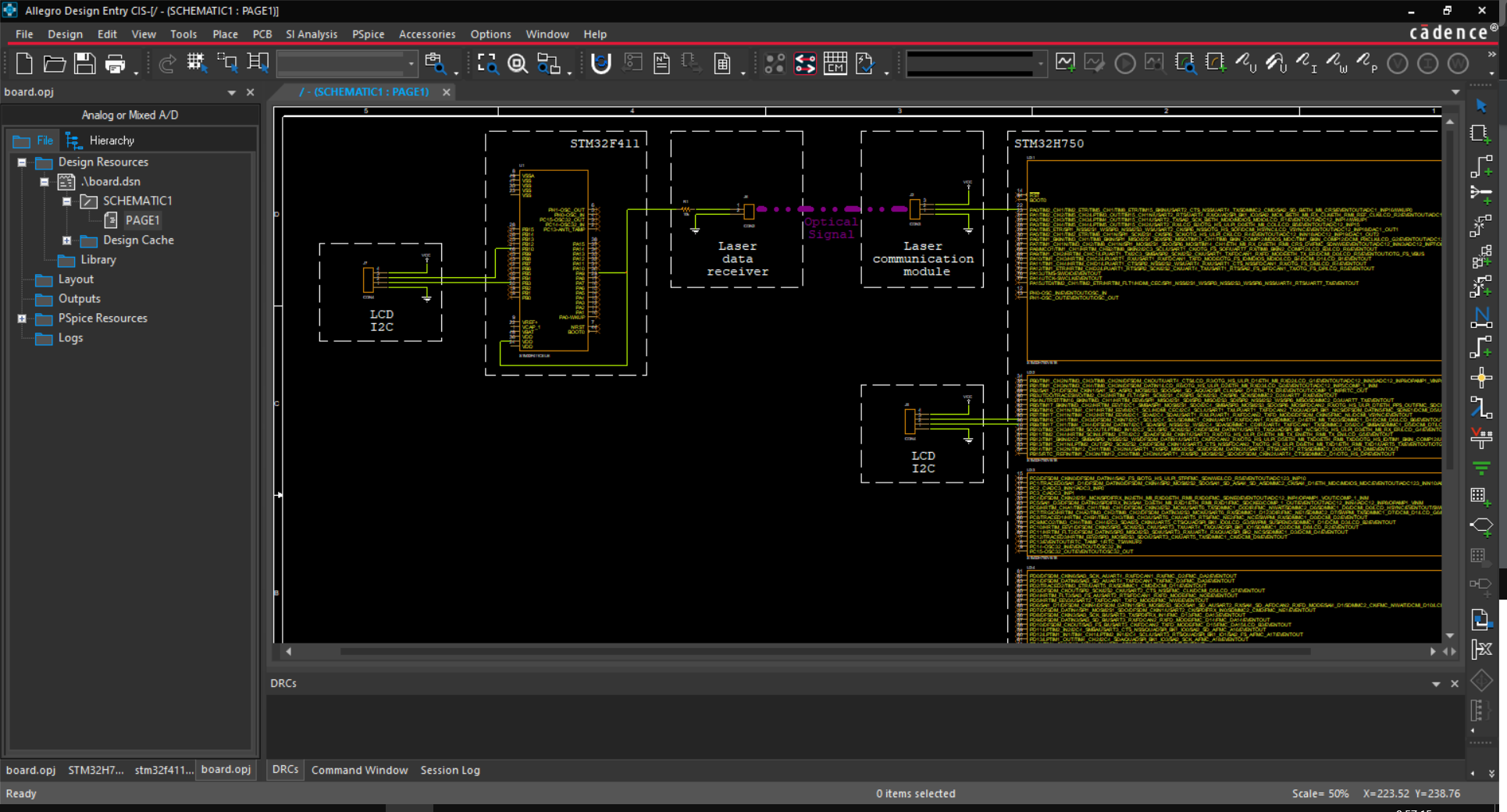


Рисунок 5 – Электрическая схема устройства спроектированная в Cadence Allegro Design CIS

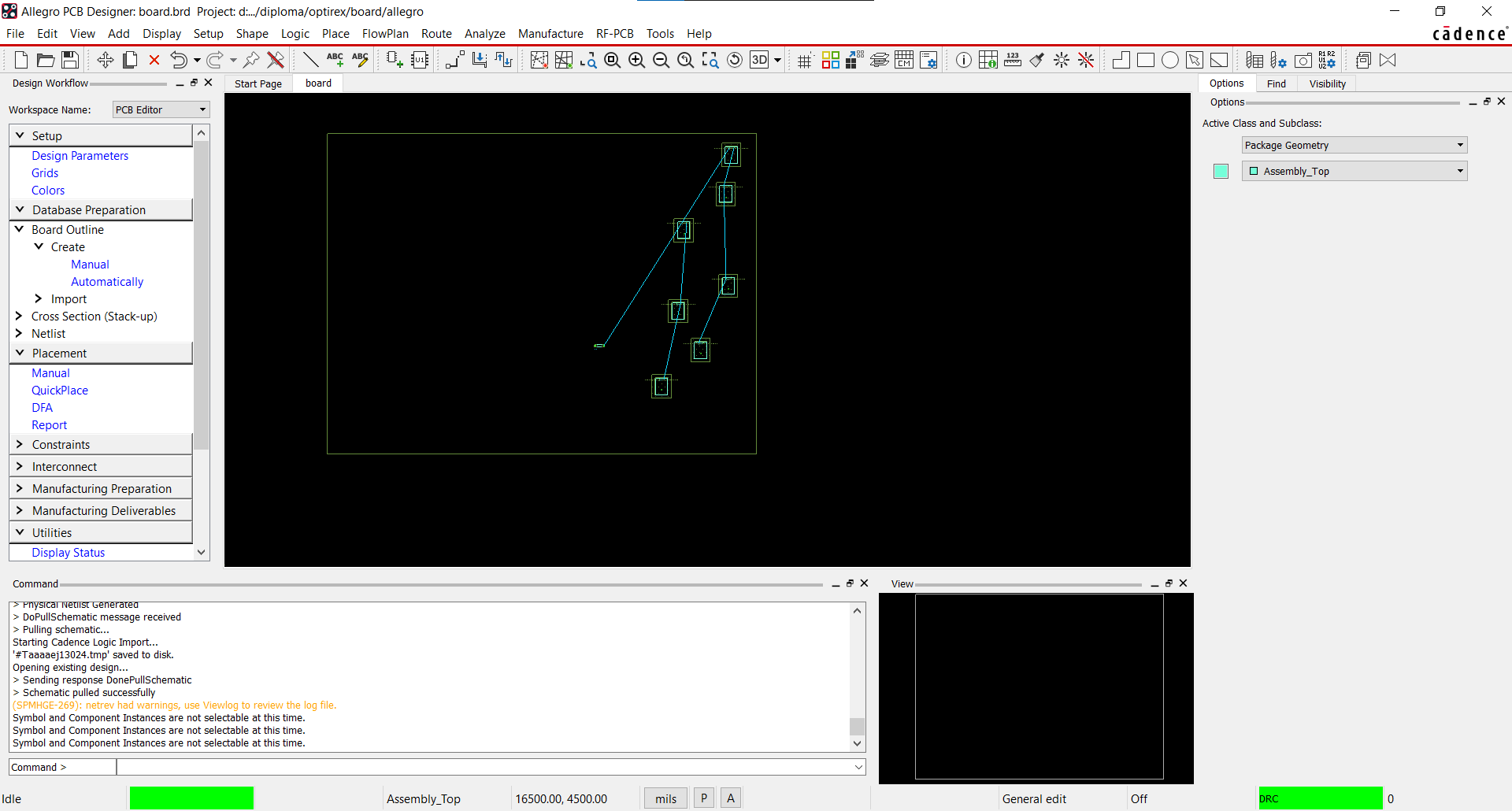
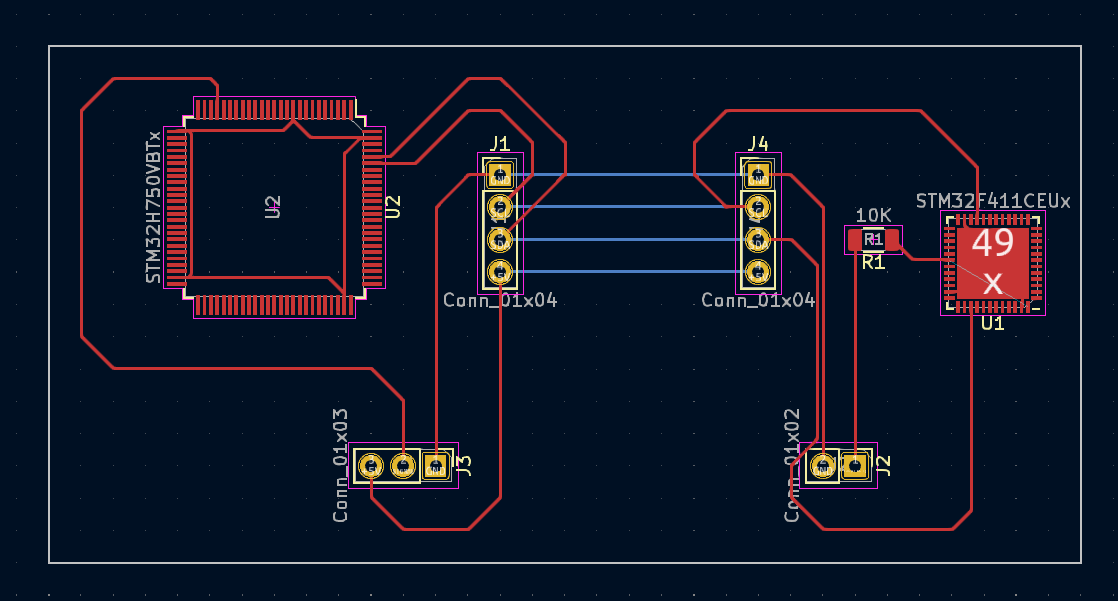


Рисунок 6 – Печатная плата на основе созданной электрической схемы Cadence Allegro PCB Designer

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].

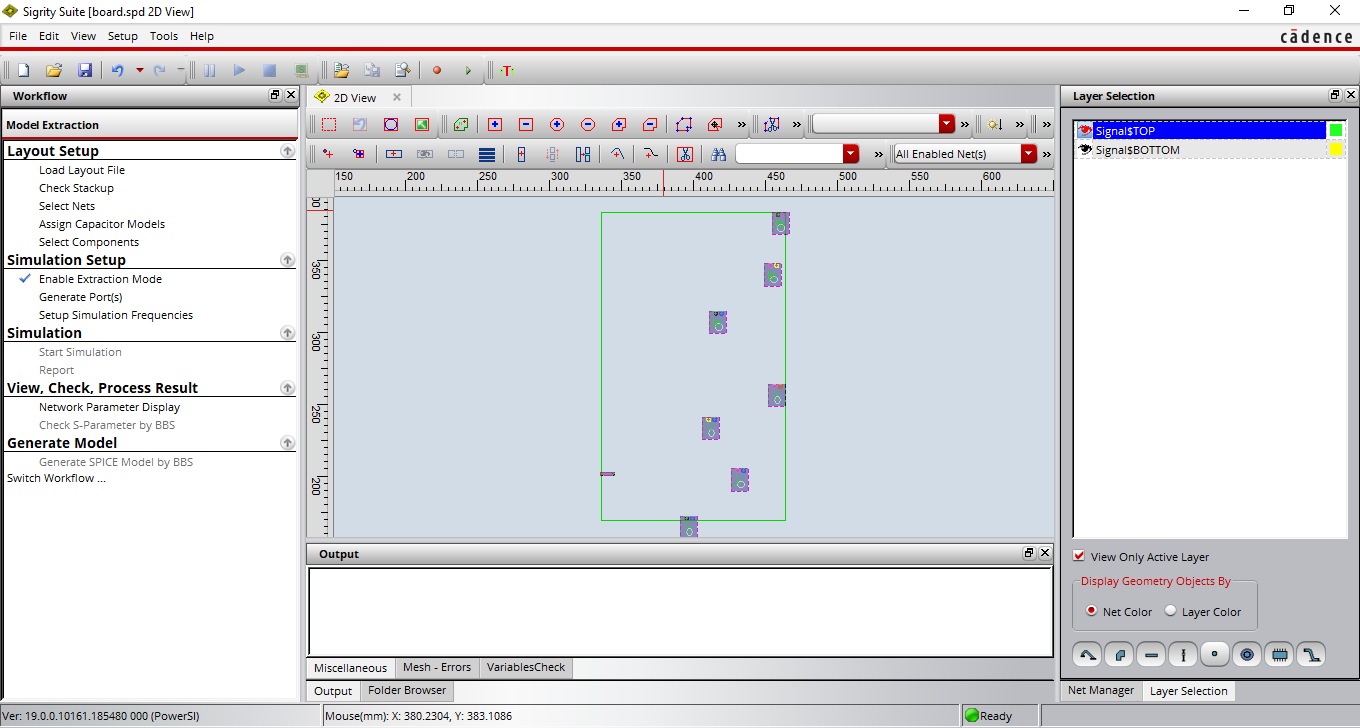


Рисунок 7 – Анализ печатной платы в Cadence Sigrity 2019 PowerSI

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).



Рисунок 8 – Проведение ассимиляционных тестов на макетном стенде с применением электроизмерительных приборов и устройств



Рисунок 9 – Проведение ассимиляционных тестов на макетном стенде с применением электроизмерительных приборов и устройств

**1.3. Исправление неисправностей, возникших при проектировании печатной платы**

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).

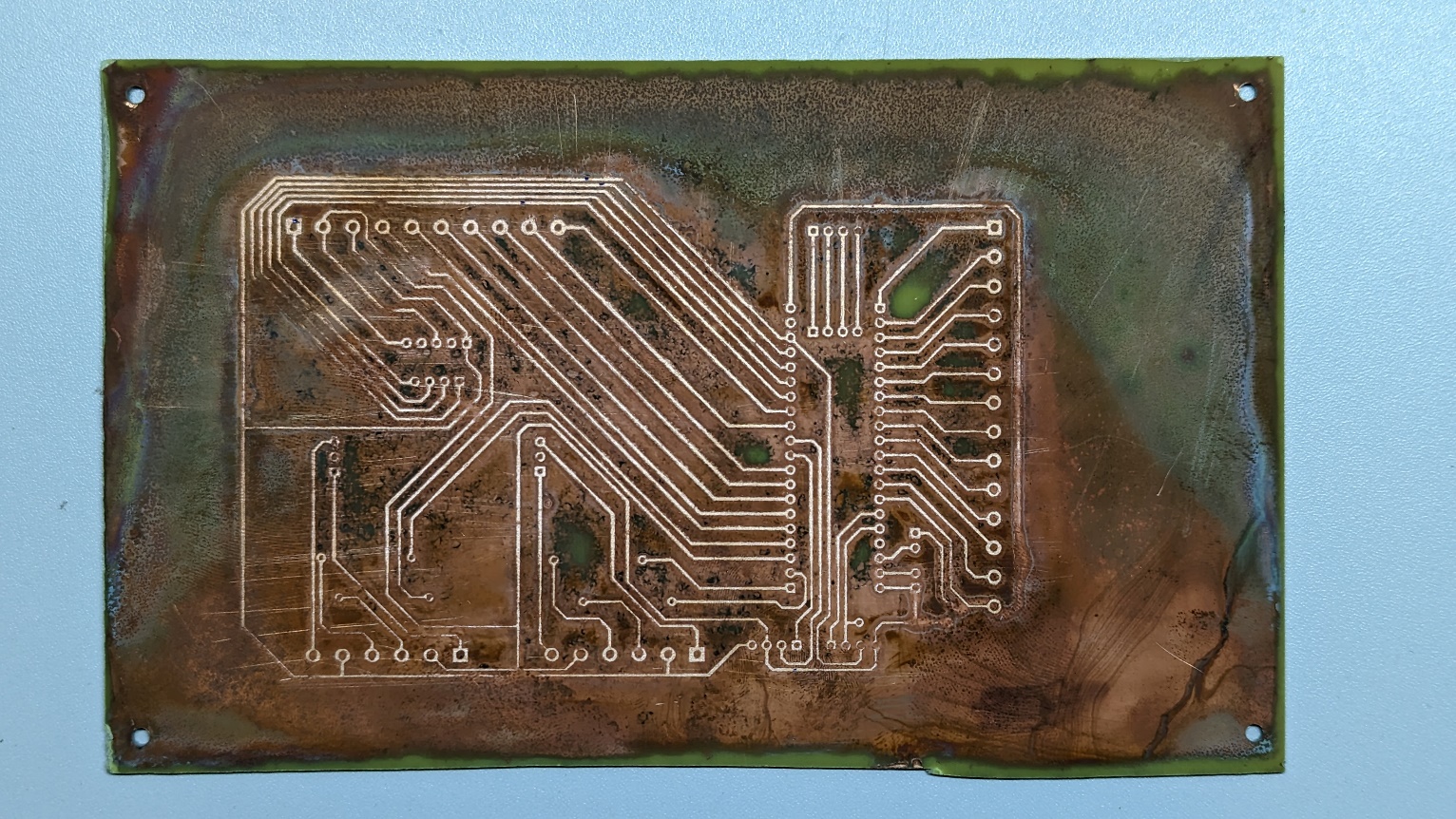


Рисунок 10 – Первая версия печатной платы устройства

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.

**Глава 2. Программное обеспечение комплекса**

**2.1. Программное окружение для создания встраиваемых приложений**

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.

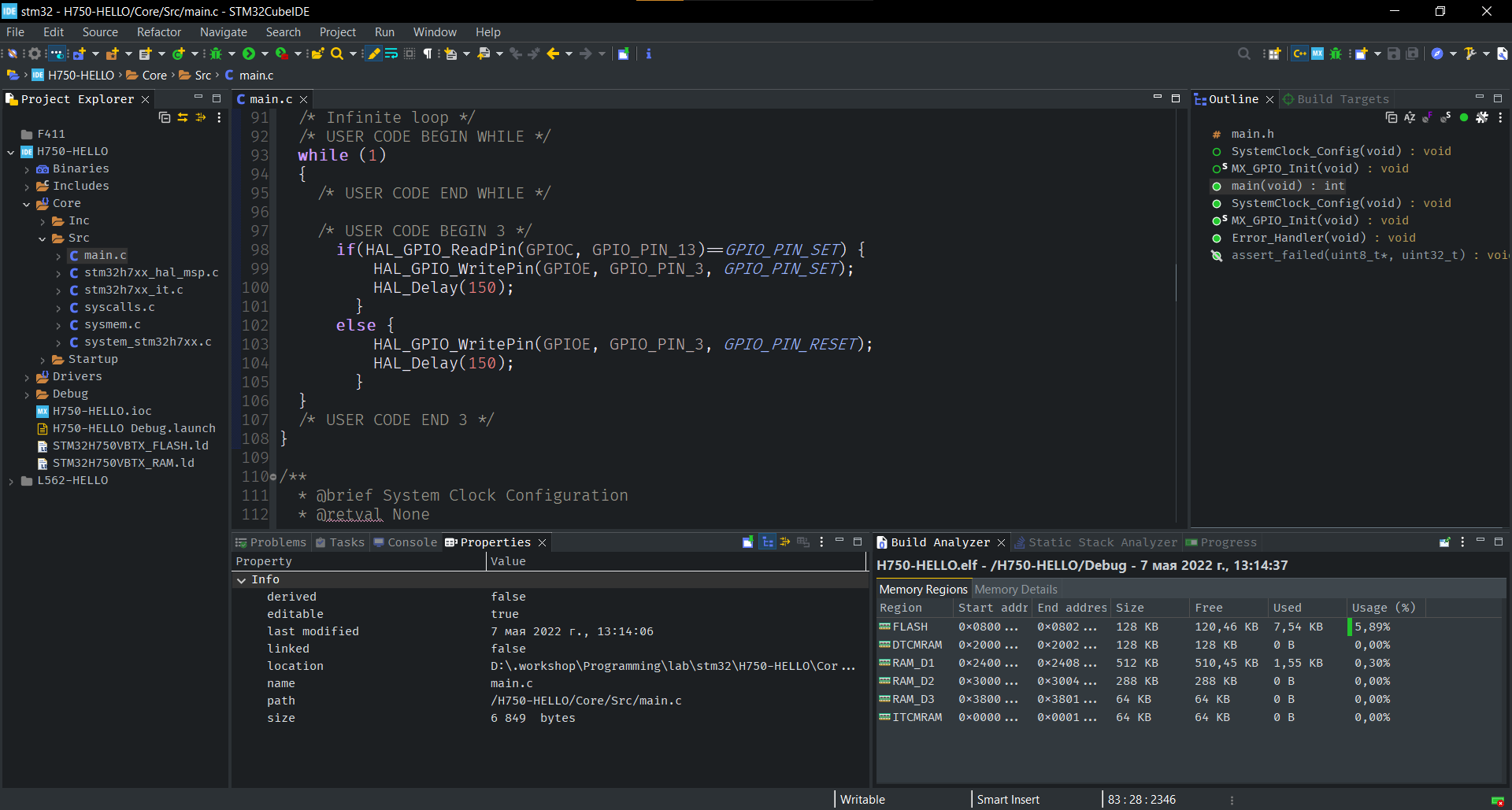


Рисунок 12 – Разработка и отладка программного кода встраиваемых систем на основе микроконтроллера ARM промышленного стандарта с использованием IDE STM32CubeIDE

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].

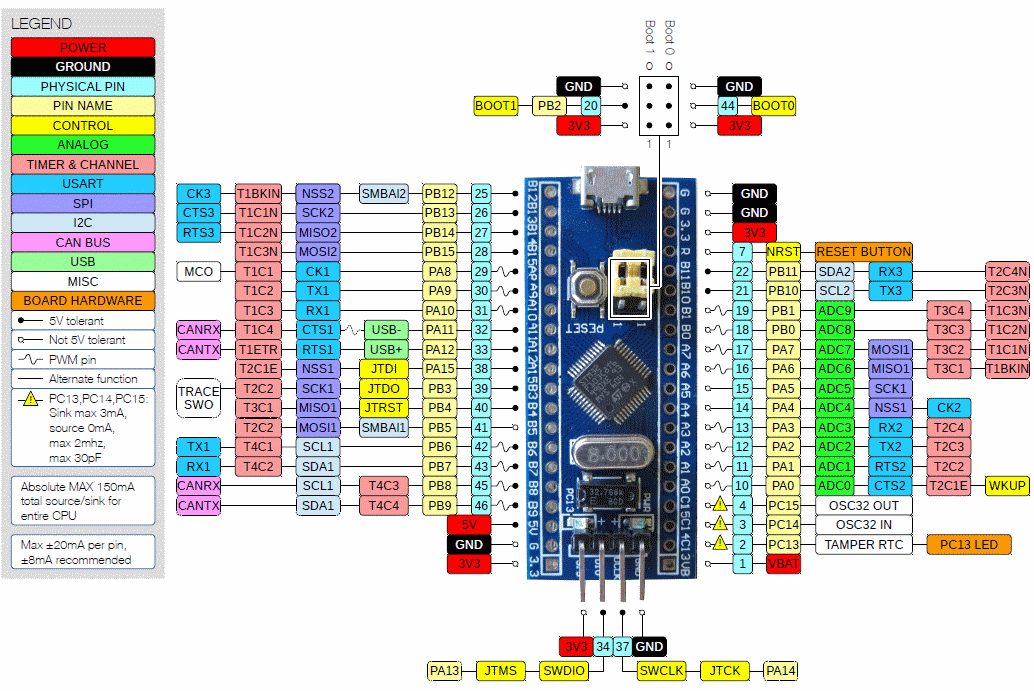


Рисунок 15 – Микроконтроллер STM32F103C8T6

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.

**2.2. Оптимизация программного кода с учетом возможностей микроконтроллера**

Молниеносное развитие сетевых технологий, сподвигло многих компаний и людей задуматься над безопасность передаваемой, отправляемой и хранимой информацией. Существует огромное количество приложений, которые по определению должны обеспечивать высокую степень защиты данных. Это касается Интернета вещей (см. Рисунок 16), терминалов оплаты, банкоматов, счетчиков коммунальных услуг, систем безопасности и многих других. При этом в каждом из перечисленных случаев необходимо защитить данные не только от кражи, но и от вредоносного изменения. Это достаточно сложная задача даже для статистической математики.

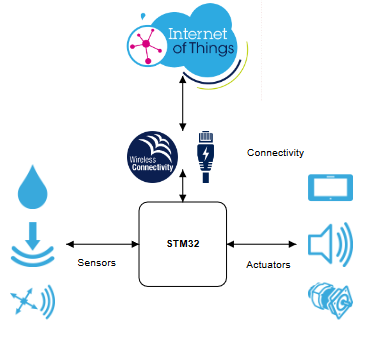


Рисунок 16 – Составная схема базового устройства Интернета вещей на базе микроконтроллера STM32

В июля 2016 года компания STMicroelectronics презентовала свою фирменную библиотеку шифрования для надежного хранения и защиты информация непосредственно на микроконтроллерах. Библиотека была выпущена в качестве программного расширения для фирменной интегрированной среды разработки STM32CubeIDE. Библиотека имеет сертифицированную поддержку следующих алгоритмов:

* Криптографические алгоритмы серии AES с разрядностью 128, 192, и 256 в режимах ECB, CBC, CTR, CFB, OFB, CCM, GCM, CMAC, KEY WRAP, XTS.
* Хеш-функции с поддержкой режима HMAC серии SHA с разрядностью 1, 224, 256, 384, 512.
* Программный генератор случайных чисел на базе DRBG-AES-128.
* Создание и хранение цифровых ключей по стандарту RSA с поддержкой протокола PKCS-1v1.5 с режимами кодирования/декодирования и хранения цифровой подписи.
* Генерация и хранения ключей по стандарту ECC с режимами Scalar multiplication и ECDSA [8].

Кроме того, библиотека имеет несертифицированную поддержку дополнительных алгоритмов ARC4, DES, TripleDES (ECB (Electronic Codebook Mode) и CBC (Cipher-Block Chaining)), хеш-функции (MD5 и HKDF-SHA-512), ChaCha20, Poly1305, CHaCHA20-POLY1305, ED25519, Curve25519. Схему работы криптографического сопроцессора можно увидеть на Рисунке 17.

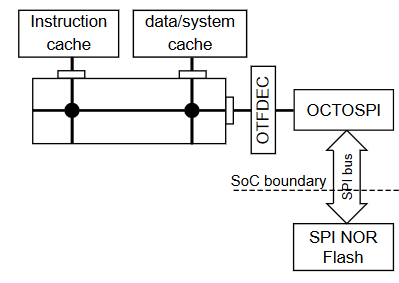


Рисунок 17 – Схема работы криптографического сопроцессора на базе микроконтроллера STM32

**Глава 3. Разработка криптографического алгоритма и адаптация алгоритма под аппаратно-программные требования комплекса**

**3.1. Криптографический алгоритм AES-256**

AES-256 (Advanced Encryption Standard) — это криптографический алгоритм симметричного шифрования, который используется для защиты данных и обеспечения их конфиденциальности. Он был разработан Национальным институтом стандартов и технологий (на англ. NIST) США и является одним из самых безопасных алгоритмов шифрования на сегодняшний день. Криптографический алгоритм AES-256 использует в своей основе 256-битный ключ для шифрования данных, что обеспечивает высокий уровень защиты по сравнению с другими алгоритмами, например DES и TDES. Каждый блок данных обрабатывается отдельно, что делает алгоритм надежным и защищенным от атак типа "человек посередине" (с англ. – man-in-the-middle).

Разработчики криптографического алгоритма заложили в структура алгоритма понятие высокой безопасности с помощью табличных массивов зашифрованных и не зашифрованных данных, при этом, злоумышленник, который располагает большой вычислительной мощностью может использовать атаку на криптографический алгоритм с помощью метода перебора ключа (brute force attack) или атака по времени выполнения (timing attack). Поэтому особенно важно использовать дополнительные меры безопасности, такие как двухфакторная аутентификация и защита от несанкционированного аппаратного считывания прошивки и данных из Flash-памяти.

На сегодняшний день, AES-256 является одним из самых надежных алгоритмов шифрования в мире, который обеспечивает высокий уровень защиты данных. Он используется в различных сферах, где требуется защита конфиденциальных данных, и является важным инструментом для обеспечения безопасности в современном мире.

Криптографический алгоритм AES-256 может быть реализован на микроконтроллере STM32 с помощью специальных библиотек, таких как STM32 X-CUBE CRYPTOLIB. Эта библиотека содержит набор функций для шифрования и расшифровки данных с использованием AES-256.

Однако, при использовании алгоритма AES-256 на микроконтроллере STM32 любой серии, необходимо учитывать ограниченные ресурсы микроконтроллер - объем оперативной и постоянной памяти, а также производительность микроконтроллера в вычислениях операций с плавающей точкой. Поэтому важно оптимизировать код и выбирать подходящие параметры алгоритма для конкретной прикладной задачи.

**3.2. Оптимизация алгоритма AES-256**

Проводя различные исследования и эксперименты с программным кодом, я выделил несколько пунктов об оптимизации криптографического алгоритма для использования в микроконтроллере STM32. Оптимизация алгоритма AES-256 для микроконтроллера STM32F1/F4/H7 может быть выполнена с помощью следующих методов:

1. *Выбор правильных параметров алгоритма.* AES-256 имеет несколько параметров, например количество раундов и размер ключа, которые могут быть настроены для оптимизации производительности. В качестве примера скажу, что уменьшение количества раундов может ускорить процесс шифрования, но может снизить уровень безопасности.
2. *Использование аппаратного ускорения*. Многие микроконтроллеры STM32 имеют аппаратное ускорение для криптографических операций, включая AES-256. Использование аппаратного ускорения может значительно ускорить процесс шифрования и расшифровки данных (см. Рисунок 18).
3. *Оптимизация кода*. Оптимизация кода может включать в себя использование более эффективных алгоритмов или структур данных, уменьшение количества операций и использование более быстрых функций.
4. *Управление памятью*. Управление памятью может быть оптимизировано для уменьшения нагрузки на микроконтроллер и ускорения процесса шифрования. Например, использование буферов фиксированного размера может снизить количество операций выделения и освобождения памяти.
5. *Использование асинхронных операций*. Использование асинхронных операций может позволить микроконтроллеру выполнять другие задачи во время процесса шифрования или расшифровки данных (см. Рисунок 19).
6. *Оптимизация выборки ключей*. Выборка ключей может быть оптимизирована для уменьшения нагрузки на микроконтроллер и ускорения процесса шифрования. Например, использование кэша ключей может снизить количество операций выборки ключей.

|  |  |
| --- | --- |
|  |  |
| Рисунок 18 – Архитектура ядра STM32H750VBT6 | Рисунок 19 – Архитектура ядра STM32F411CEU6 |

**3.3. Использование аппаратных средств защиты информации**

Микроконтроллеры STM32 являются важным элементом современных систем автоматизации и управления. Однако, при использовании этих устройств возникает необходимость обеспечения безопасности программного кода и данных, хранящихся во встроенной Flash-памяти. Для этого разработчики микроконтроллера STM32 предусмотрели механизмы защиты на уровне аппаратуры и программного обеспечения.

Один из таких механизмов – защита области памяти (*Memory Protection Unit, MPU*), который позволяет разделить память на несколько областей и задать права доступа к каждой из них. Это позволяет защитить программный код и данные от несанкционированного доступа и изменения (см. Рисунок 20).

*Memory Protection Unit (MPU)* — это механизм защиты памяти на уровне аппаратуры, который позволяет разделить память на несколько областей и задать права доступа к каждой из них. Это позволяет защитить программный код и данные от несанкционированного доступа и изменения.

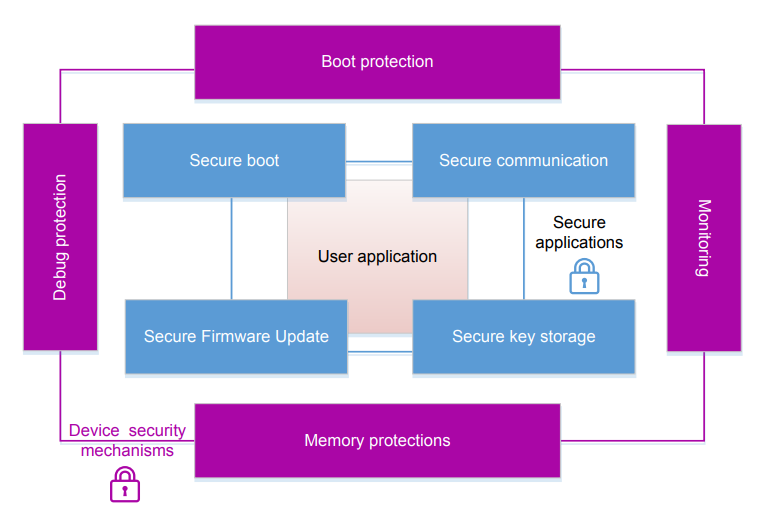


Рисунок 20 – Уровни аппаратно-программной защиты информации в микроконтроллерах серии STM32

MPU работает на уровне железа и может быть настроен для ограничения доступа к определенным областям памяти для чтения, записи или выполнения. Например, можно разрешить чтение программного кода, но запретить его запись или выполнение из области данных. Для настройки MPU используются специальные регистры, которые задают параметры защиты для каждой области памяти. Кроме того, в микроконтроллерах STM32 есть возможность использовать MPU в сочетании с механизмом защиты от записи, что позволяет еще более усилить защиту данных Flash-памяти (см. Рисунок 21).

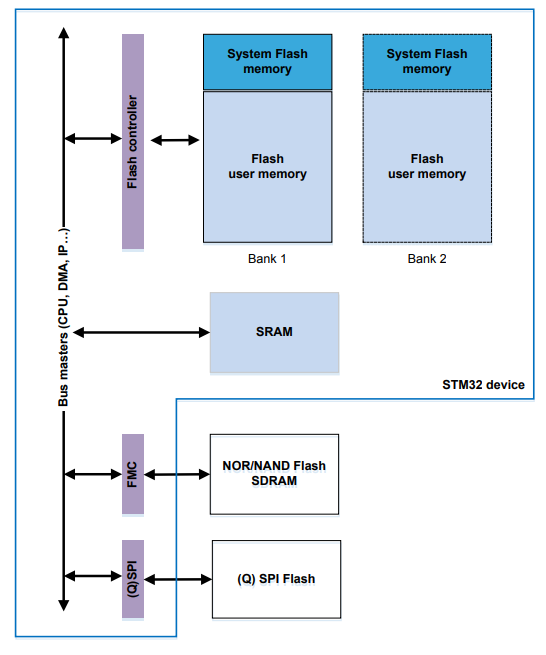


Рисунок 21 – Защита информации с использованием механизмов защиты Flash-памяти

Кроме того, микроконтроллеры STM32 имеют механизм защиты от записи (*Write Protection*), который позволяет запретить запись в определенные области памяти. Это может быть полезно для защиты программного кода от изменений после его загрузки в устройство.

Для настройки защиты Flash-памяти в STM32 используется специальный инструментарий – *STM32CubeMX* и *STM32CubeProg*. С их помощью можно задать параметры защиты, такие как права доступа к областям памяти и уровень защиты от записи.

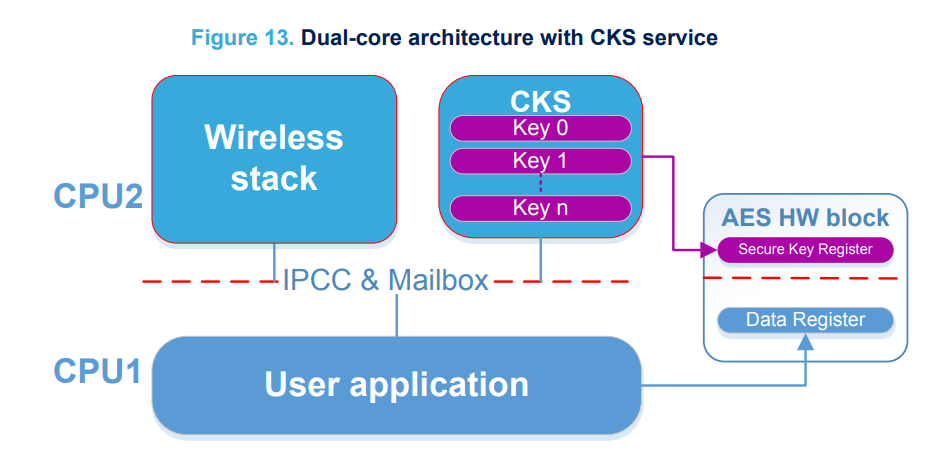


Рисунок 22 – Защита информации с помощью аппаратного блока ускорения криптографических операций

Защита данных Flash-памяти в микроконтроллере STM32 является важным аспектом обеспечения безопасности программного кода и данных. Она особенно важна для устройств, работающих в критических условиях или хранящих конфиденциальную информацию как в случае с трансляцией зашифрованной информации по инфракрасному оптическому каналу связи.

**Заключение**

Рассмотренные на практике средства защиты компьютерной  
информации касательно применения таких средств на микроконтроллерных платформах семейства ARM и STM32, конечно же, не закрывают весь спектр угроз безопасности информации.

Кроме этого, всегда следует помнить, что методы и средства  
осуществления угроз безопасности информации постоянно совершенствуются. С развитием систем обработки и передачи данных появляются новые виды угроз. Поэтому постоянное развитие претерпевают и системы защиты информации. Наряду с этим источники угроз ведут систематический поиск новых уязвимостей в существующих пользовательских приложения, информационных службах и системах защиты.

Все это говорит о том, что современному специалисту необходимо постоянно обновлять и расширять свои знания о существующих угрозах, уязвимостях и современных средствах, и методах обеспечения информационной безопасности.

Важно понимать, что защита информации не ограничивается  
техническими методами. Большое количество угроз  
несанкционированного доступа к конфиденциальной информации могут быть  
реализованы по причине неправильной работы пользователей компьютерной  
системы вследствие незнания основ сетевой безопасности. Защита информации включает в себя кроме технических мер еще и обучение или правильный подбор обслуживающего персонала.

Помимо этого, защита должна постоянно совершенствоваться вместе с  
развитием компьютерной сети. Опасно недооценивать и так называемые внутренние угрозы информационно-технологического типа, обусловленные действиями легальных пользователей корпоративной системы.

При проектировании, разработке, создании и отладке систем защиты информации и устройств на их базе, следует учитывать возможные негативные последствия злонамеренных действий авторизированных пользователей.

В настоящее время обобщенная теория безопасности информации пока не создана. Применяемые на практике подходы и средства нередко страдают  
недостатками и не обладают объявленной надежностью. Поэтому необходимо  
обладать достаточной подготовкой и квалифицированно ориентироваться во  
всем спектре вопросов обеспечения информационной безопасности, понимая  
их комплексный и взаимообусловленный характер.

Во время прохождения практики подкрепил полученные во время учебы теоретические навыки практическими. Познакомился с организацией, структурой и принципами принцип работы предприятия. Развил коммуникативные навыки в области индивидуальной и командной работы. Получил опыт работы в коллективе.

Во время прохождения практики показал себя, как способного и ответственного сотрудника. Выполнял задания качественно и своевременно.

Научился разрабатывать, проектировать, отлаживать и использовать методы защиты информации в приложения для встраиваемых систем.

Я стал ответственным, терпеливым и думаю хорошим специалистом, что нельзя было сказать обо мне до этого. Данная практика является хорошим практическим опытом для дальнейшей самостоятельной профессиональной деятельности. Я освоил несколько аппаратных и программных технологий, а также закрепил знания в нескольких смежных областях науки, производства и инженерии.

**Список использованных источников**

# 1. K. Mitzner, Complete PCB Design Using OrCAD Capture and PCB Editor – Second Edition. –Elseiver Academic Press, 2019ю – 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. Новелло К., Освоение STM32 / пер. с англ. Д. Карасев. – М.: Leanpub Publishing, 2018. – 826 с.

# 6. Novello C., Mastering STM32 – Second Edition. - М.: Leanpub Publishing, 2022. – 910 с.

# 7. AN5156 Application Note – Introduction to STM32 microcontrollers security., 2019. – 55 с.

# 8. Владимиров С.М., Габидулин Э.М., Колыбельников А.И., Кшевецкий А.С., Криптографические методы защиты информации. – М.: Издательство Московского Государственного Университета, 2021. – 433 с.

# 9. 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.

# 10. Белоус А.И., Солодуха В.А., Основы кибербезопасности. – М: Техносфера, 2021. – 482 с.