Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ **ИНФОРМАТИКА И СИСТЕМЫ УПРАВЛЕНИЯ**

КАФЕДРА **КОМПЬЮТЕРНЫЕ СИСТЕМЫ И СЕТИ (ИУ6)**

НАПРАВЛЕНИЕ ПОДГОТОВКИ **09.03.03 ПРИКЛАДНАЯ ИНФОРМАТИКА**

Вычислитель SHA-256

Техническое задание на курсовую работу
по дисциплине Схемотехника

Листов 4

Студент гр. ИУ6-64Б _____ С.П.Пантелеев
(Группа) (Подпись, дата) (И.О. Фамилия)

Руководитель курсовой работы, (кандидат технических наук) _____ О.Ю.Ерёмин
(Подпись, дата) (И.О. Фамилия)

Москва, 2020

1 ВВЕДЕНИЕ

Настоящее техническое задание распространяется на разработку «Вычислителя SHA-256», именуемого в дальнейшем «устройством». Данное устройство предназначено для расчета результатов выполнения внутреннего цикла алгоритма хеширования SHA-256. Устройство необходимо выполнить на основе ПЛИС.

Вычислитель используется при вычислении контрольных сумм от данных для последующего обнаружения в них ошибок, при выработке электронной подписи.

2 ОСНОВАНИЯ ДЛЯ РАЗРАБОТКИ

Устройство разрабатывается на основе учебного плана кафедры ИУ6 «Компьютерные системы и сети» Московского государственного технического университета им. Н.Э.Баумана.

3 ЦЕЛИ И ЗАДАЧИ

3.1. Цель работы

Целью курсового проектирования является разработка вычислителя результатов выполнения внутреннего цикла хеш-функции SHA-256.

3.2. Решаемые задачи

3.2.1. Анализ технического задания и возможных путей решения поставленной задачи.

3.2.2. Обоснование и синтез электрической функциональной схемы устройства.

3.2.3. Выбор элементной базы на основании технических требований.

3.2.4. Разработка электрической принципиальной схемы устройства.

3.2.5. Построение временных диаграмм.

3.2.6. Расчет параметров мощности устройства.

4 ТРЕБОВАНИЯ К РАЗРАБАТЫВАЕМОМУ УСТРОЙСТВУ

4.1. Требования к составу и параметрам технических средств

4.1.1. Количество информационных входов - 7, информационных выходов - 6.

4.1.2. Разрядность информационных входов и выходов - 32.

4.1.3. Устройство реализуется на базе ПЛИС..

4.1.4. Тактовая частота – 10 МГц.

4.1.5. Мощность потребления – не более 3 Вт.

4.2. Требования к эксплуатации

4.2.1. Условия эксплуатации в соответствие с СанПиН2.2.2/2.4.1340-03.

4.3. Требования к маркировке и упаковке

Требования к маркировке и упаковке не предъявляются.

4.4. Требования к транспортированию и хранению

Требования к транспортировке и хранению не предъявляются.

5 ОПИСАНИЕ РАБОТЫ УСТРОЙСТВА

Устройство должно рассчитывать результаты выполнения внутреннего цикла хеш-функции SHA-256. В начале каждого раунда хеширования (каждые 64 итерации внутреннего цикла) на информационные входы подаются новые значения вспомогательных переменных, запись которых в память устройства обеспечивается соответствующим управляющим сигналом. В ходе каждой итерации на седьмой информационный вход подается фрагмент информационного сообщения. Расчет результатов итерации выполняется по положительному фронту тактирующего сигнала. Результаты вычислений записываются в память устройства в следующем такте.

6 ТРЕБОВАНИЯ К ДОКУМЕНТАЦИИ

6.1 В состав сопровождающей документации должны входить:

6.1.1 Расчетно-пояснительная записка на 25 – 30 листах формата А4;

6.1.2 Техническое задание;

6.1.3 Спецификация.

6.2 Графическая часть должна быть включена в расчетно-пояснительную записку в качестве приложений и иллюстраций:

6.2.1 Временные диаграммы;

6.2.2 Схема электрическая структурная;

6.2.3 Схема электрическая функциональная;

6.2.4 Схема электрическая принципиальная.

7 СТАДИИ И ЭТАПЫ РАЗРАБОТКИ

Таблица 1 – Этапы разработки

№	Название этапа	Срок, % выполнения	Отчетность
1	Исследование предметной области	1 – 4 нед., 15%	Описание общего принципа работы устройства.
2	Разработка технического задания	5 нед., 20%	Техническое задание
3	Проектирование и разработка функциональной электрической схемы	6 – 7 нед. 40%	Функциональная схема
4	Проектирование и разработка принципиальной электрической схемы	8 – 10 нед. 60%	Принципиальная схема
5	Оформление расчетно-пояснительной записки	11 – 14 нед. 90%	Расчетно-пояснительная записка
6	Защита курсовой работы	15 – 16 нед., 100%	Доклад (3 – 5 минут)

8 ПОРЯДОК КОНТРОЛЯ И ПРИЕМА

8.1 Порядок контроля

Контроль выполнения осуществляется руководителем еженедельно.

8.2 Порядок защиты

Защита осуществляется перед комиссией, состоящей из преподавателей кафедры ИУ6.

8.3 Срок защиты

Срок защиты: 15-16 недели.

9 ПРИМЕЧАНИЕ

В процессе выполнения работы возможно уточнение отдельных требований технического задания по взаимному согласованию руководителя и исполнителя.