|  |  |
| --- | --- |
|  | **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 **09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА**

**РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

***К КУРСОВОЙ РАБОТЕ***

***НА ТЕМУ:***

***«Вычислитель SHA-256»***

Студент \_\_ИУ6-62Б\_\_\_\_\_\_\_ **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_С.В. Астахов\_\_\_\_\_\_**

(Группа) (Подпись, дата) (И.О. Фамилия)

Руководитель курсовой работы **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_Т.А.\_Ким\_\_\_\_\_\_\_\_\_**

(Подпись, дата) (И.О. Фамилия)

*2022 г.*

и

ЗАДАНИЕ

РЕФЕРАТ

Записка 21 стр., 7 рис., 3 табл., 4 источника, 2 прил.

СХЕМОТЕХНИКА, ЭВМ, SHA-256, ХЕШ-ФУНКЦИЯ, ПЛИС, FPGA, ВЫЧИСЛИТЕЛЬ, VERILOG, XILINX.

Объектом разработки является устройство, производящее расчет внутреннего цикла алгоритма хеширования SHA-256.

Цель работы – эскизный проект цифрового устройства ограниченной сложности.

При проектировании решены следующие задачи: анализ объекта разработки на функциональном уровне, разработка функциональной схемы устройства, выбор ПЛИС для реализации устройства, описание устройства на языке Verilog, синтез RTL-схемы устройства, разработка принципиальной схемы обвязки ПЛИС, расчет электрических параметров.

Результатом разработки является проект на языке Verilog, предназначенный для загрузки в ПЛИС, и набор конструкторской документации.

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ, СОКРАЩЕНИЯ

ТЗ — техническое задание.

САПР — система автоматизированного проектирования.

ПЛИС — программируемая логическая интегральная схема.

Мультиплексирование с разделением по времени — технология аналогового или цифрового мультиплексирования, в котором несколько сигналов или битовых потоков передаются одновременно как подканалы в одном коммуникационном канале.

ВВЕДЕНИЕ

В данной работе производится разработка проекта устройства, производящего расчет внутреннего цикла алгоритма хеширования SHA-256.

Устройство должно рассчитывать заданную часть алгоритма SHA-256 в соответствии со стандартом [1].

Так как для одной итерации алгоритма необходим большой объем данных, необходимо использовать мультиплексирование с разделение по времени. Также, в силу сложности устройства, целесообразно разрабатывать его, применяя язык описания аппаратуры [2].

Хеш-функции, в том числе SHA-256, применяются главным образом для вычисления контрольных сумм, работы с электронной подписью и построения уникальных идентификаторов для наборов данных. Широкое применение хеш-функций в современных информационных системах обуславливает актуальность разработки [3].

**1. Анализ требований**

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

[1] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[2] <https://www.ispras.ru/proceedings/docs/2008/15/isp_15_2008_7.pdf>

[3] http://89.250.84.46/physics-mathematics/article/view/2552/2506