

План

Научный руководитель:

Тренькаев Вадим Николаевич

Тема:

Реализация на ПЛИС криптографических алгоритмов

Семестр 1

1. Реализация перестраиваемого автомата на подстановках с помощью VHDL
2. Реализация различных способов задания подстановки (замены)
3. Оценка параметров реализации
 - a. Быстродействие (тактовая частота)
 - b. Ресурсоёмкость (количество использованных LUT, CLB, логических вентилях)
4. Реализация перестраиваемого автомата на подстановках с использованием результатов из п.2.

Семестр 2

1. Реализация задания подстановок с криптографическими свойствами.
2. Оценка параметров реализации
3. Применение реализации из п.1 в перестраиваемом автомате.