

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего
образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра системного анализа и автоматического управления

Отчет по заданию 3. Вариант 29

Студента 3 курса 321 группы направления 09.03.01 ИВТ

Факультета компьютерных наук и информационных технологий

Чесакова Максима Евгеньевича

Задача №1 Транзитивна ли заданная функция $h : \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$? Решить задачу аналитически, затем проверить с помощью программной реализации транзитивность по модулю 256.

$$h(x) = (x \oplus 1) \oplus (2(x \wedge (1 + 2x) \wedge (3 + 4x) \wedge (7 + 8x) \wedge (15 + 16x) \wedge (31 + 32x) \wedge (63 + 64x))) \oplus (4(x^2 + 29))$$

Аналитическое решение.

Теорема Ларина. Многочлен F с целыми или рациональными 2-адическими коэффициентами биективен (транзитивен) на \mathbb{Z}_2 , тогда и только тогда, когда F биективен (транзитивен) по модулю 4, т. е. редукция $F \bmod 4$ является перестановкой (транзитивен по модулю 8, т. е. редукция $F \bmod 8$ одноцикловая перестановка)

Ответ: .

Программная реализация на Python.