

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИ ЛАБОРАТОРНОЙ РАБОТЫ №6**

**В РАМКАХ ДИСЦИПЛИНЫ «МЕТОДЫ И СРЕДСТВА КРИПТОРГАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»**

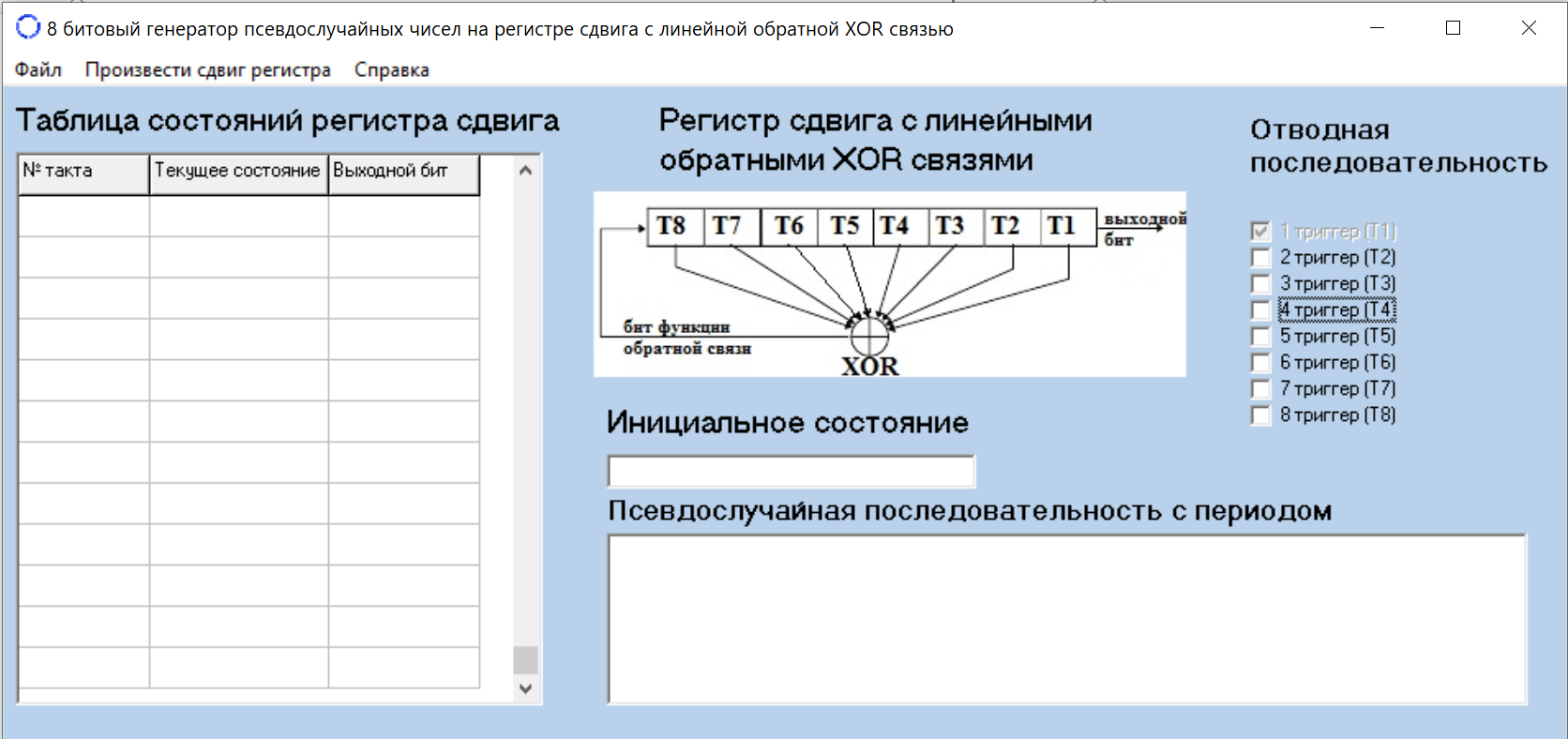
Выполнил:

Студент 3-ого курса

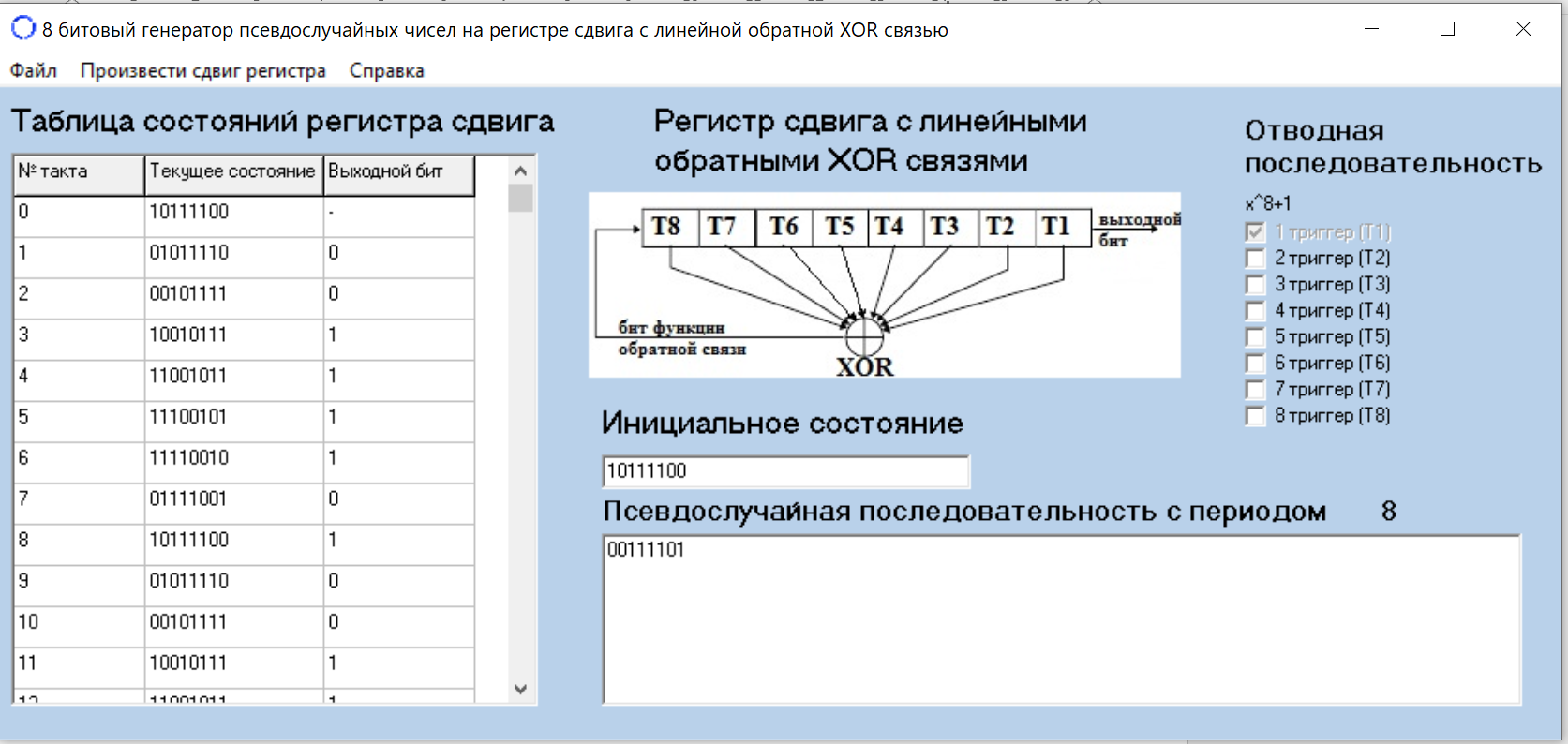
Учебной группы БИСО-02-22

Зубарев В.С.

Цель работы: Изучение работы регистра сдвига с линейной обратной связью.

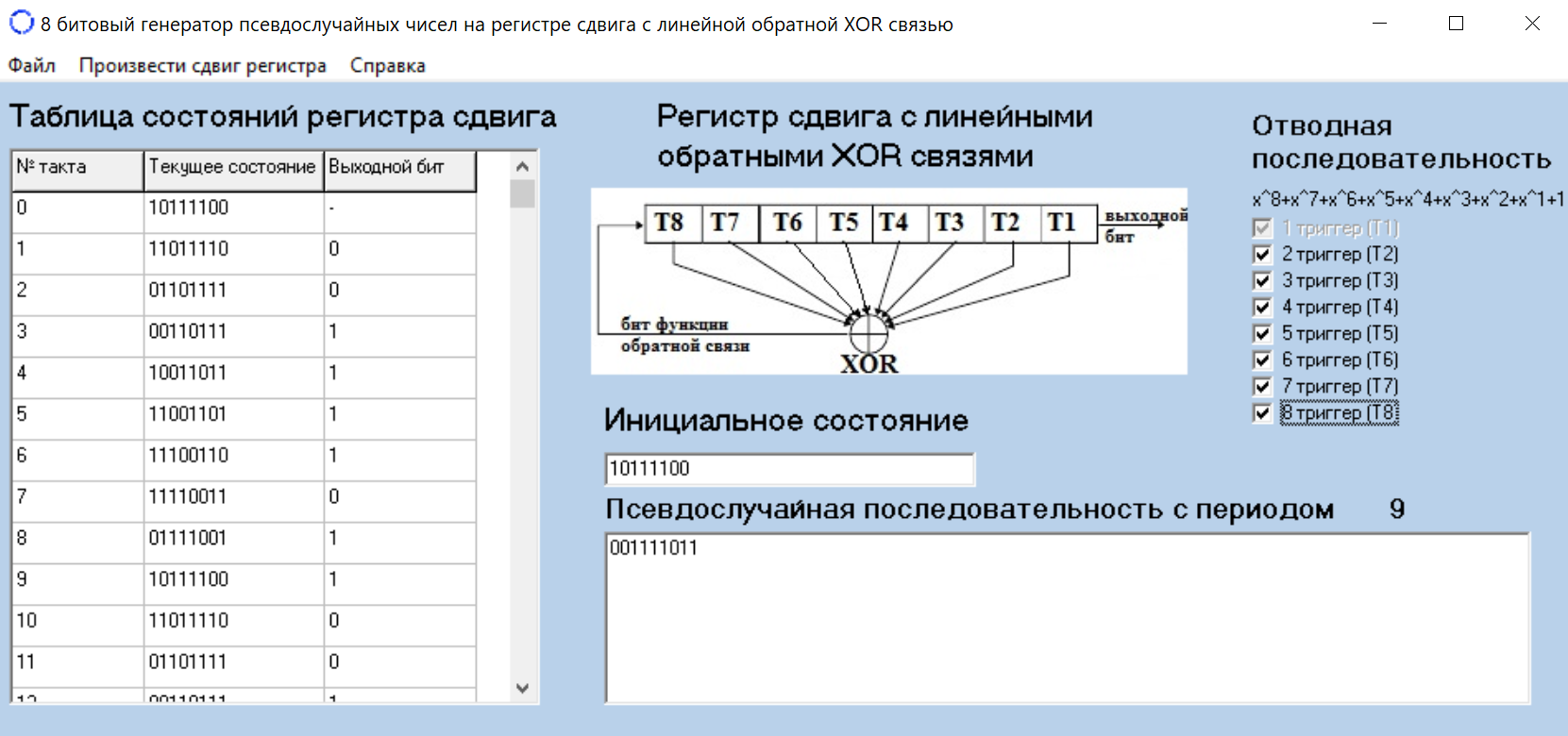
Исходное состояние программы  


1.Введите в поле «Инициальное значение» любое восьмиразрядное двоичное число. Установите отводную последовательность (по умолчанию обязательно один триггер должен входить в отводную последовательность и должна присутствовать хотя бы одна обратная связь, иначе регистр будет неисправен). Нажмите пункт меню «Произвести сдвиг регистра».



Данная псевдослучайная последовательность не является максимальной, так как для 8-битного РгСсЛОС максимальная длинна последовательности 255.

2.Выполните п. 3—5 с теми же параметрами, но в отводной последовательности укажите только один триггер. Ответьте на вопрос: какое значение поступает на вход восьмого триггера при каждом его сдвиге и как оно вычисляется в случае, если присутствует одна обратная связь? Если присутствует две или более (до восьми) обратных связей?



На данном рисунке видно, что выбраны все регистры для обратной связи. Это значит, что новый старший бит будет генерироваться путем сложения по модулю два всех значений в регистре. Рассмотрим, как на такте 2 генерируется входной бит для такта 3.

.   
Для шага 2.

Общая формула для отводной последовательности

где a = {0,1} для 1 … n, a xi указывает разряд.

В нашем случае n = 8, а период псевдослучайной последовательности n+1= 9

Такт 1

Выходной бит будет получен в такте 10 – 0

Такт 2

Выходной бит будет получен в такте 11 – 0

Такт 3

Выходной бит будет получен в такте 12 – 1

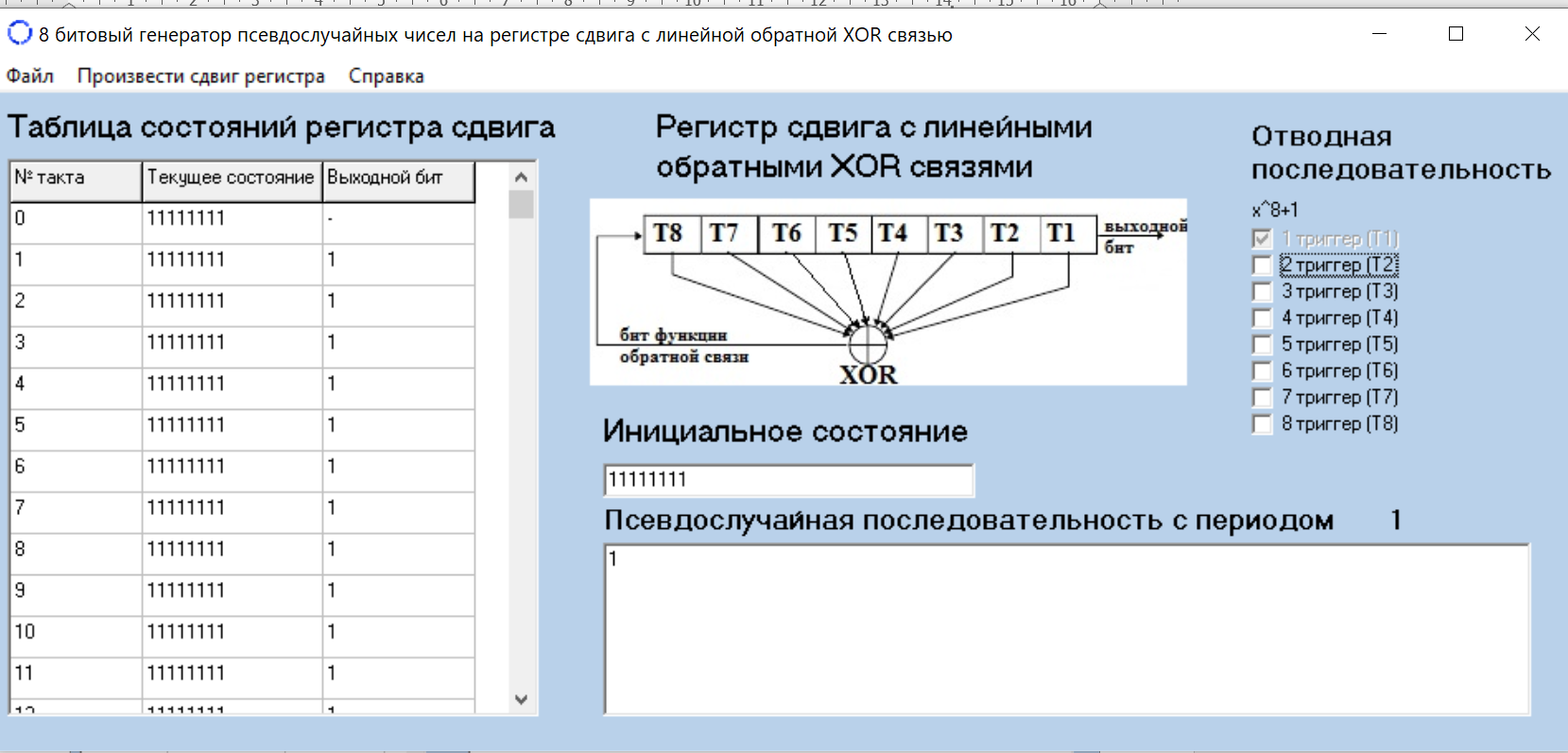
Такт 4

Выходной бит будет получен в такте 13 – 1

Такт 5

Выходной бит будет получен в такте 14 – 0

7. Выполните п. 3—5 с теми же параметрами, но в качестве инициальной последовательности укажите «11111111».

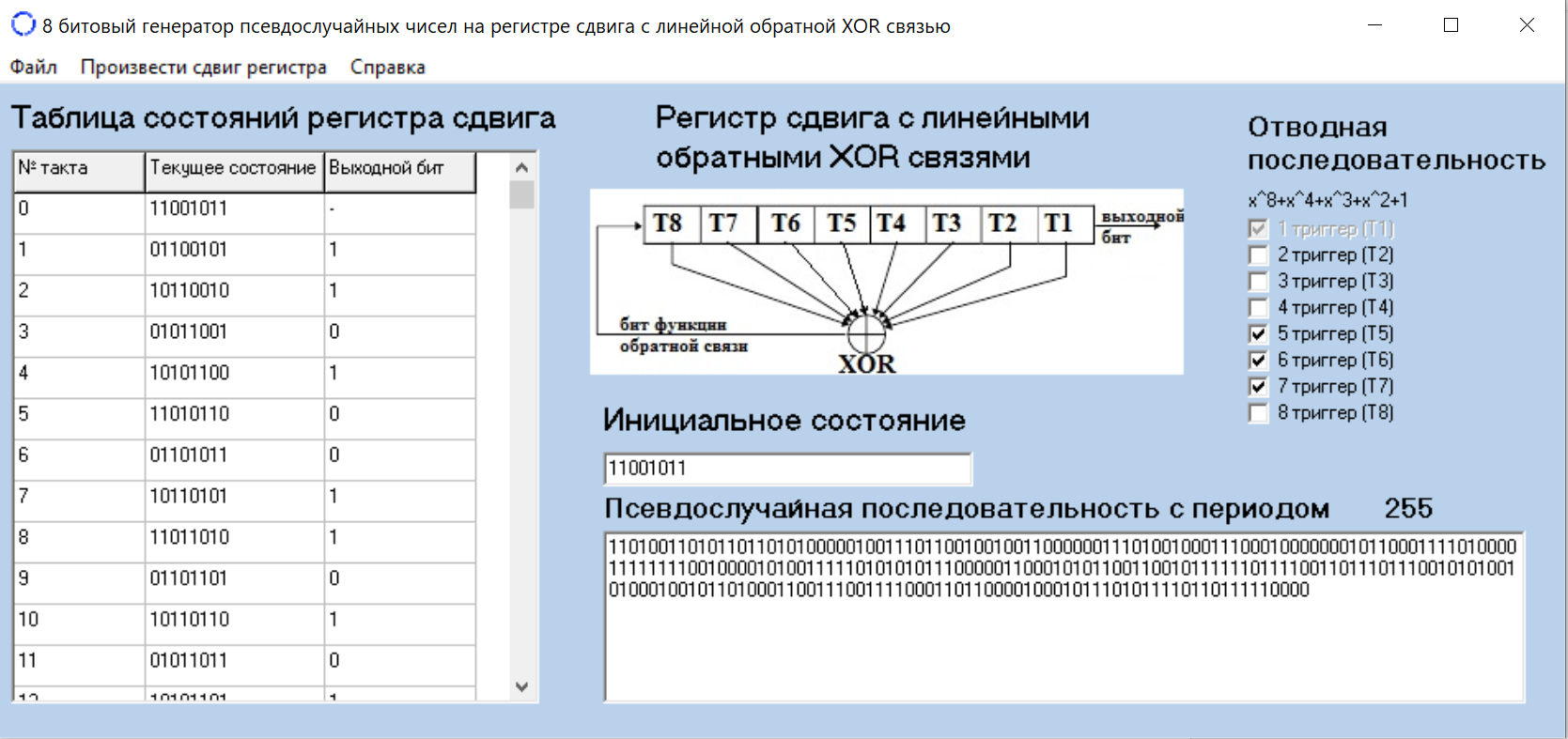


Как видно из рисунка при вводе 11111111, как инициальное состояние для РгСсЛОС, при установке нечетного количества регистров (1,3,5,7) для обратной связи – псевдослучайная последовательность будет иметь длину 1. Это связано с логикой сложения по модулю 2. Для нечетного количества операций XOR выводом всегда будет 1.

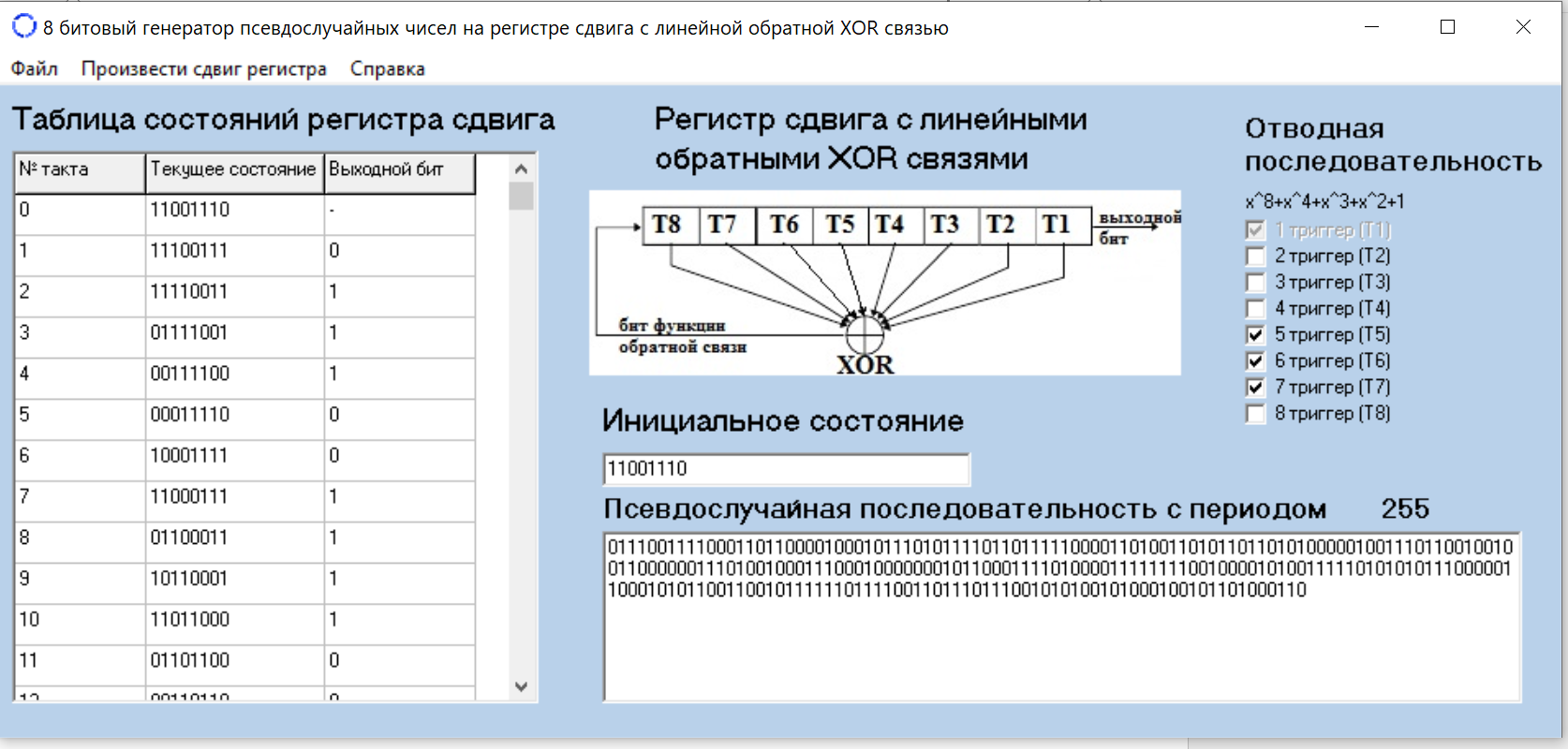
8. Выполните п. 3—5 с теми же параметрами, но в качестве инициальной последовательности укажите «00000000».  
Данное начальное состояние недопустимо при работе с РгСсЛОС, так как не имеет возможности сформировать псевдослучайную последовательность пр любом наборе триггеров для обратной связи.

9. Выполните п. 3—5, но в отводной последовательности отметьте галочками 1, 5, 6 и 7 триггеры или 1, 4, 6, 8 триггеры. Измените несколько раз инициальное значение и произведите сдвиг регистра.

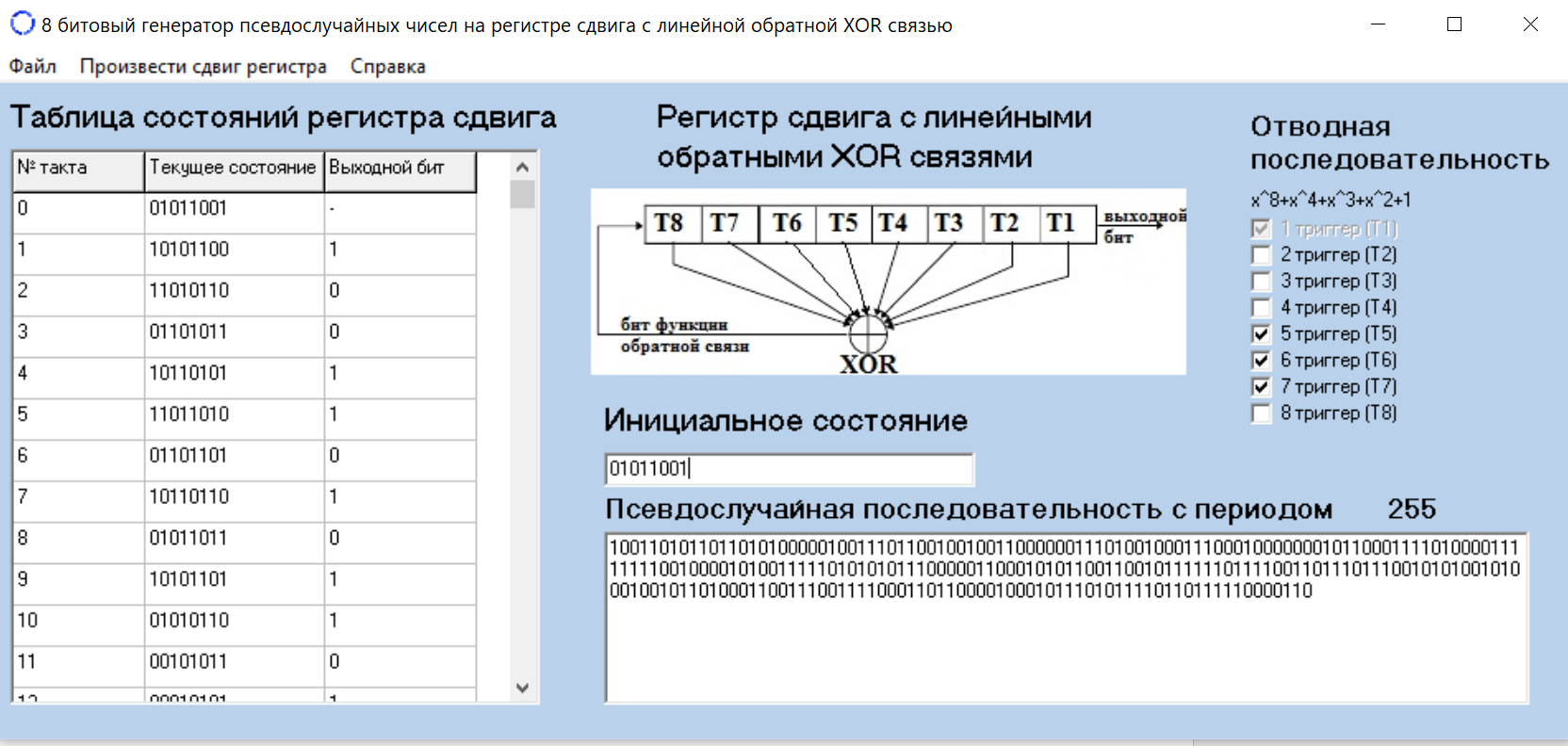
Первое значение



Второе значение



Третье значение



У всех этих значений есть одна общая черта – такая комбинация триггеров создает максимальную псевдослучайную последовательность. Это происходит потому что отводная последовательность генерируемая таким набором является примитивным многочленом, то многочленом который не может быть разложен на многочлены меньшей степени.