**Пример составления теста для лр2**

Задан полином х4 + х +1

Начальное состояние регистра 1 1 1 1:

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | **1** | **1** | **1** |
| 4 | 3 | 2 | 1 |

В обратной связи будут участвовать первая и четвертая ячейки, результат xor будет записываться в ячейку 1.

После первого такта:

Сгенерированный ключ = 1

Состояние регистра после сдвига и обратной связи 1 1 1 0

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | **1** | **1** | **0** |
| 4 | 3 | 2 | 1 |

После второго такта:

Сгенерированный ключ = 1 1

Состояние регистра после сдвига и обратной связи 1 1 0 1

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | **1** | **1** | **0** |
| 4 | 3 | 2 | 1 |

Повторяем сдвиги в зависимости от длины регистра. Минимальное количество сдвигов вычисляется по формуле: длина регистра + 20.