# **Глава 1. Теоретическая часть**

Принцип работы алгоритма Шора можно разделить на две части, которые будут рассмотрены ниже:

1. Классическое сведение разложения на множители к нахождению периода некоторой функции.
2. Квантовое нахождение периода данной функции.

## **1.1 Классическая часть алгоритма Шора**

### 1.1.1 Описание классической части алгоритма Шора

Алгоритм факторизации Шора состоит в определении простых множителей *p* и *q* для заданного числа с использованием квантовой схемы определения периода *r* некоторой периодической функции вида:

где , a – любое число, такое что и , M – число, которое необходимо факторизовать.

Рассмотрим алгоритм:

Целью рассматриваемого алгоритма является нахождение периода *r* функции , где *r* – порядок *t* по модулю M, . Необходимо выбрать число *a*,удовлетворяющее условиям, вычислить некоторые значения функции , а затем найти период данной функции. После нахождения периода необходимо, чтобы он удовлетворял следующим требованиям:

1. *r* – четное число.

Тогда . В противном случае необходимо изменить число a.

Формальное описание алгоритма:

1. Необходимо выбрать случайное число *а*, удовлетворяющее условиям: и .
2. Вычисляется период *r* функции .
3. Если период является нечетным, то необходимо вернуться на шаг назад и выбрать другое число *a*.
4. Если период является четным, то необходимо, чтобы *r* удовлетворяло следующему условию: .
5. Вычисляем .

### 1.1.2 Пример

Рассмотрим пример, где . Возьмем . Для наглядности составим таблицу функции :

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 |
|  | 1 | 2 | 4 | 8 | 16 | 11 | 1 | 2 |

Таблица 1. Функция

Из таблицы получаем, что период *r* равен 6. Полученный период удовлетворяет всем необходимым условиям. Далее находим *p* и *q* ⇒ . Получаем, что факторизация числа – .

## **1.2 Квантовая часть алгоритма Шора**