Моделирование релятивистской системы квантового распределения ключей

Дипломная работа

Большаков Роман Алексеевич
Научный руководитель: профессор,
д.ф-м.н. Молотков С.Н.

Московский государственный университет имени М.В. Ломоносова
Факультет вычислительной математики и кибернетики
Кафедра суперкомпьютеров и квантовой информатики

Москва, 2015

Структура дипломной работы

1. Введение в предметную область
2. Исследование релятивистского протокола квантового распределения ключей
3. Исследование каскадного протокола коррекции ошибок
4. Описание практической реализации и полученных результатов

Проблемы классической криптографии

Проблемы классической криптографии

- проблема обнаружения подслушивателя;

Проблемы классической криптографии

- проблема обнаружения подслушивателя;
- основанность на предположениях об ограниченности злоумышленника в средствах, мощностях, интеллекте и др.;

Проблемы классической криптографии

- проблема обнаружения подслушивателя;
- основанность на предположениях об ограниченности злоумышленника в средствах, мощностях, интеллекте и др.;
- асимметричная криптография требует бóльших вычислительных мощностей, чем симметричная;

Проблемы классической криптографии

- проблема обнаружения подслушивателя;
- основанность на предположениях об ограниченности злоумышленника в средствах, мощностях, интеллекте и др.;
- асимметричная криптография требует бóльших вычислительных мощностей, чем симметричная;
- абсолютная криптостойкость доказана только для шифрования по методу Вернама «одноразовый блокнот»;

Проблемы классической криптографии

- проблема обнаружения подслушивателя;
- основанность на предположениях об ограниченности злоумышленника в средствах, мощностях, интеллекте и др.;
- асимметричная криптография требует бóльших вычислительных мощностей, чем симметричная;
- абсолютная криптостойкость доказана только для шифрования по методу Вернама «одноразовый блокнот»;
- проблема первоначальной секретности.

Квантовое распределение ключей — механизм:

- использующий фундаментальные принципы квантовой механики,
- в результате работы которого:
  - либо получается общая для двух участников коммуникации строка случайных бит, известная только им;
  - либо происходит детектирование злоумышленника в канале связи

Актуальность релятивистского протокола

В области квантовой криптографии уже имеется много наработок и разработано достаточное число протоколов.

Актуальность релятивистского протокола

В области квантовой криптографии уже имеется много наработок и разработано достаточное число протоколов. Основные практические проблемы:

- лазеры не могут испустить ровно один фотон,

Актуальность релятивистского протокола

В области квантовой криптографии уже имеется много наработок и разработано достаточное число протоколов. Основные практические проблемы:

- лазеры не могут испустить ровно один фотон,
- потери в канале связи.

Актуальность релятивистского протокола

В области квантовой криптографии уже имеется много наработок и разработано достаточное число протоколов. Основные практические проблемы:

- лазеры не могут испустить ровно один фотон,
- потери в канале связи.

Актуальность релятивистского протокола

В области квантовой криптографии уже имеется много наработок и разработано достаточное число протоколов. Основные практические проблемы:

- лазеры не могут испустить ровно один фотон,
- потери в канале связи.

Нерелятивистские протоколы используют только ограничения квантовой механики.

Актуальность релятивистского протокола

В области квантовой криптографии уже имеется много наработок и разработано достаточное число протоколов.
Основные практические проблемы:

- лазеры не могут испустить ровно один фотон,
- потери в канале связи.

Нерелятивистские протоколы используют только ограничения квантовой механики.
Релятивистский протокол $=$ квантовая механика $+$ специальная теория относительности.

Цель дипломной работы

Целью данной дипломной работы является создание программных средств:

1. моделирования и визуализации релятивистского протокола квантового распределения ключей в открытом пространстве,
2. моделирования и визуализации каскадного протокола коррекции ошибок по аутентичному каналу.

Схема релятивистского протокола

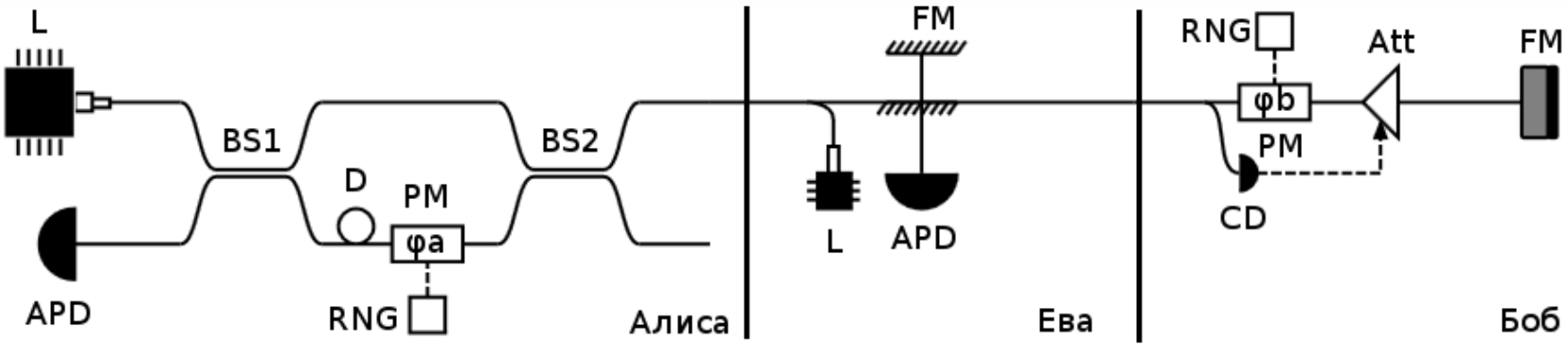


Схема релятивистского протокола

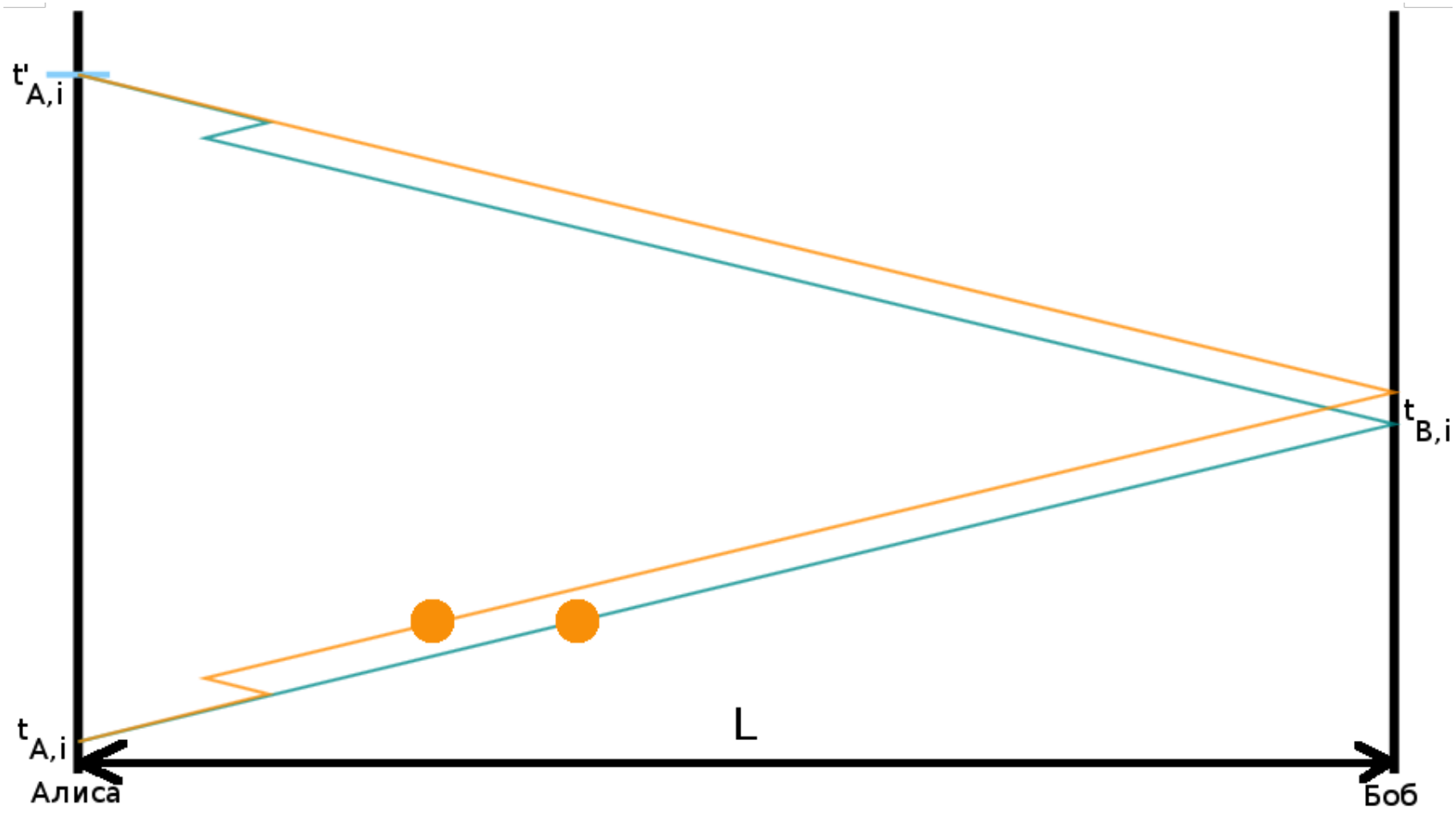
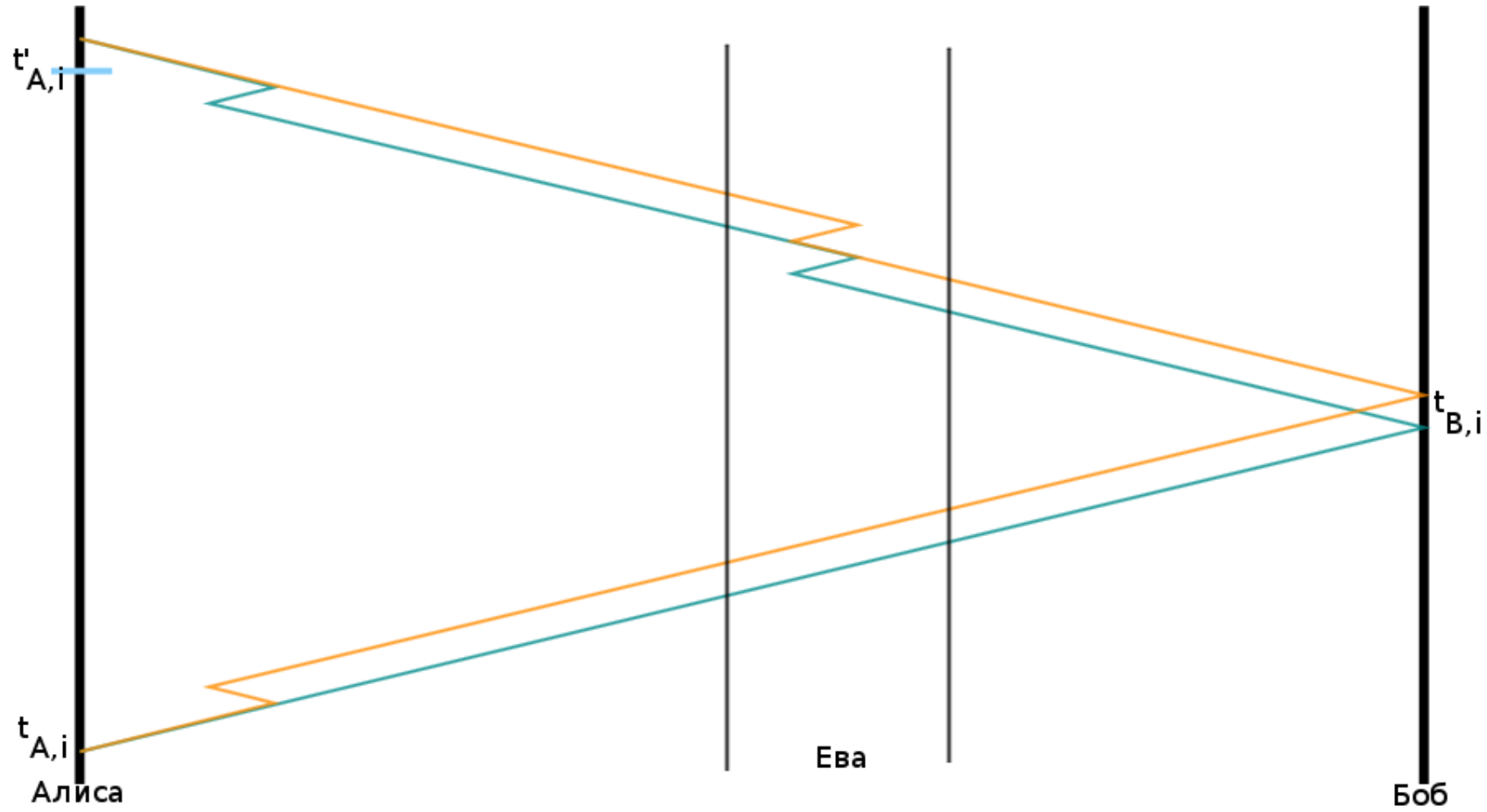


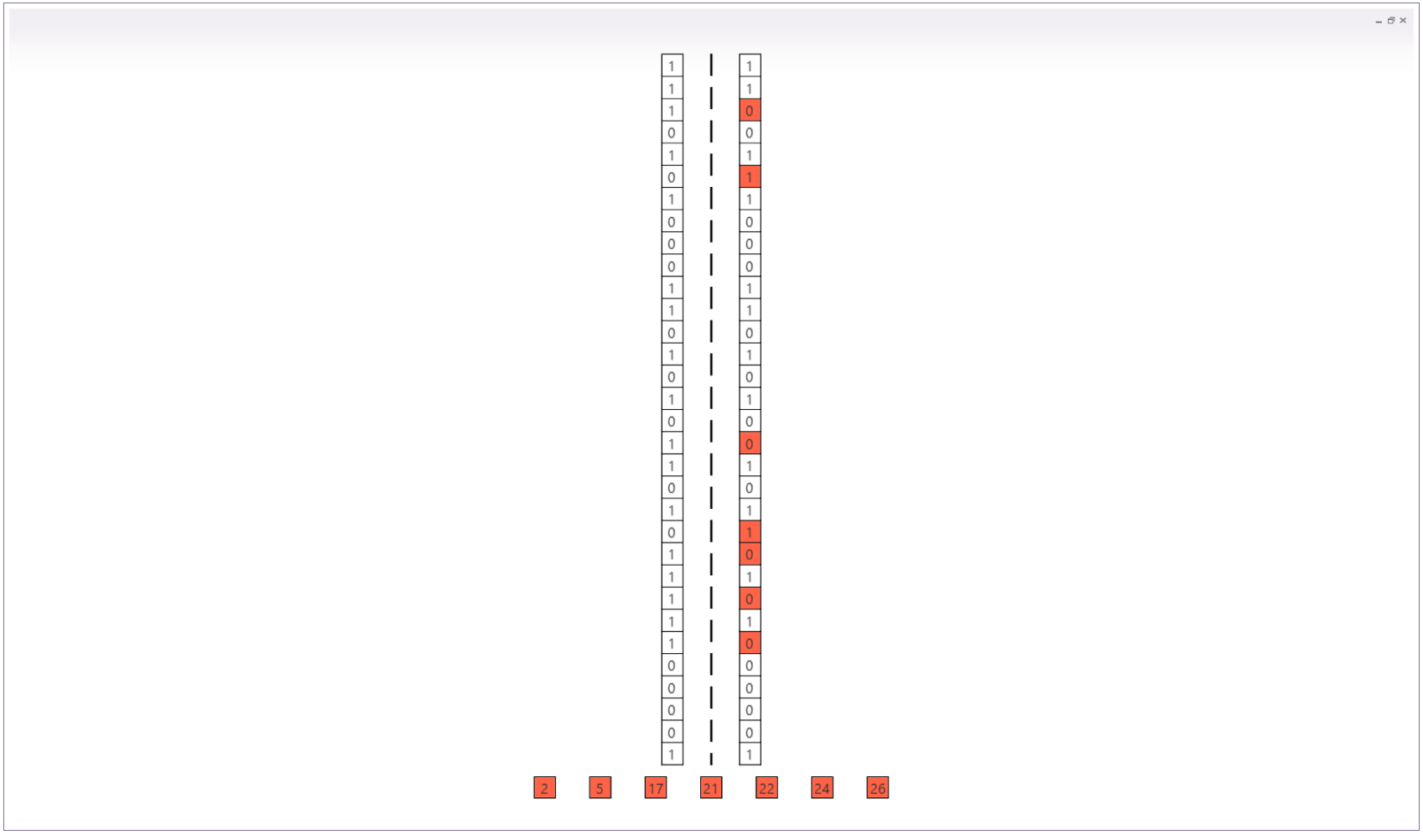
Схема релятивистского протокола



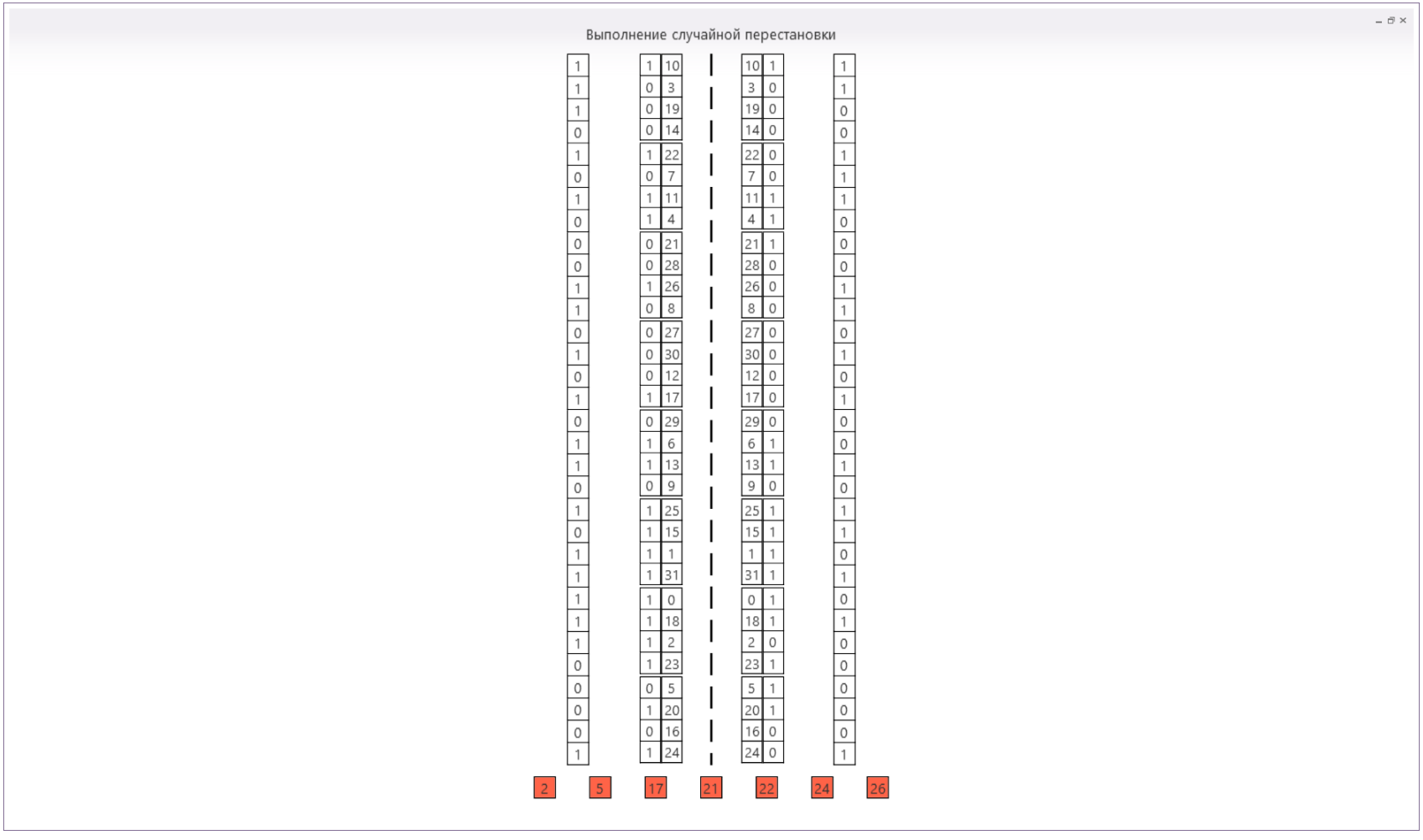
Каскадный метод коррекции ошибок

В канале связи (в частности если это открытое пространство) неизбежно присутствуют помехи, вносящие ошибки в ключ. Их необходимо исправить, выдав как можно меньше информации о ключе возможному подслушивателю.

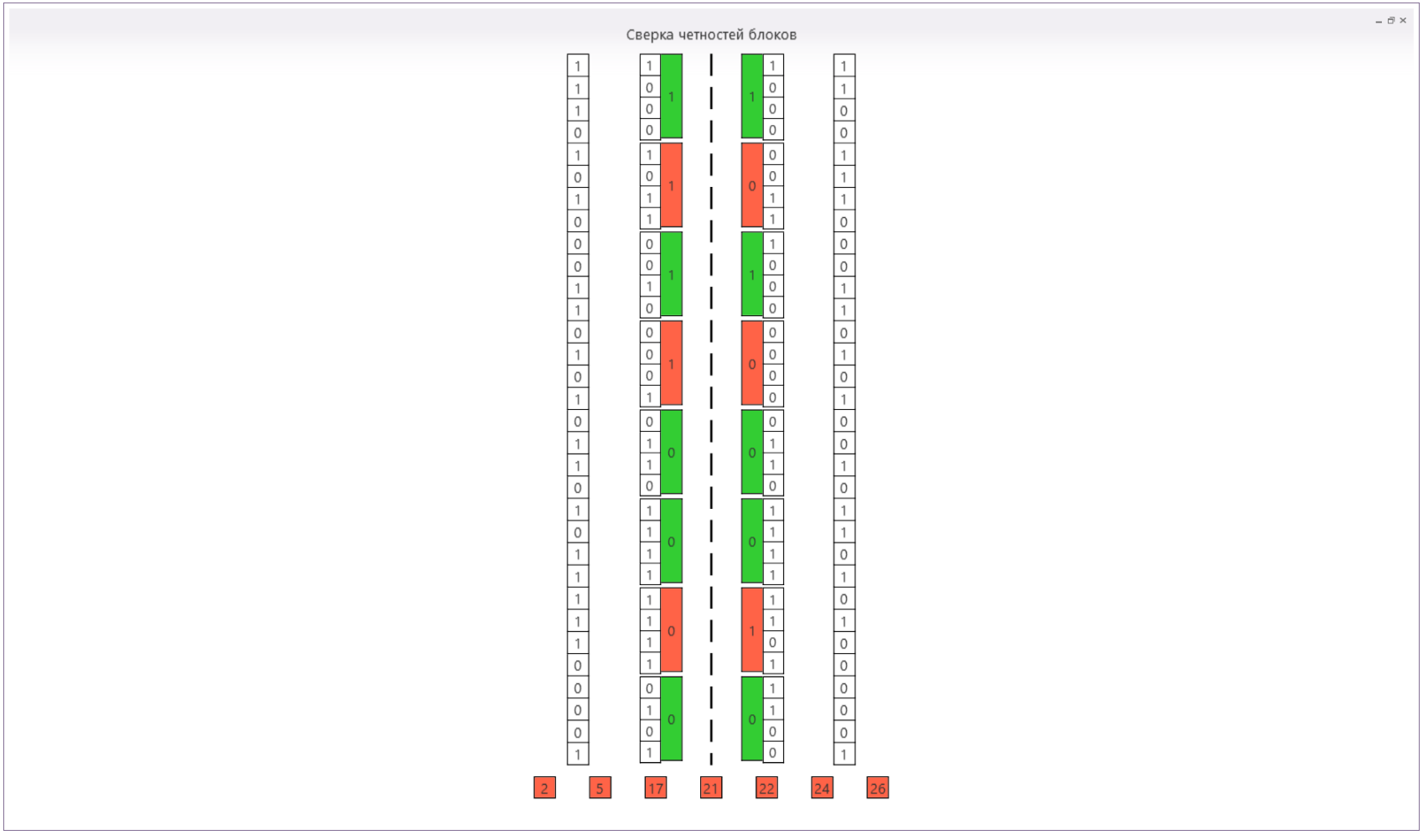
Каскадный метод коррекции ошибок



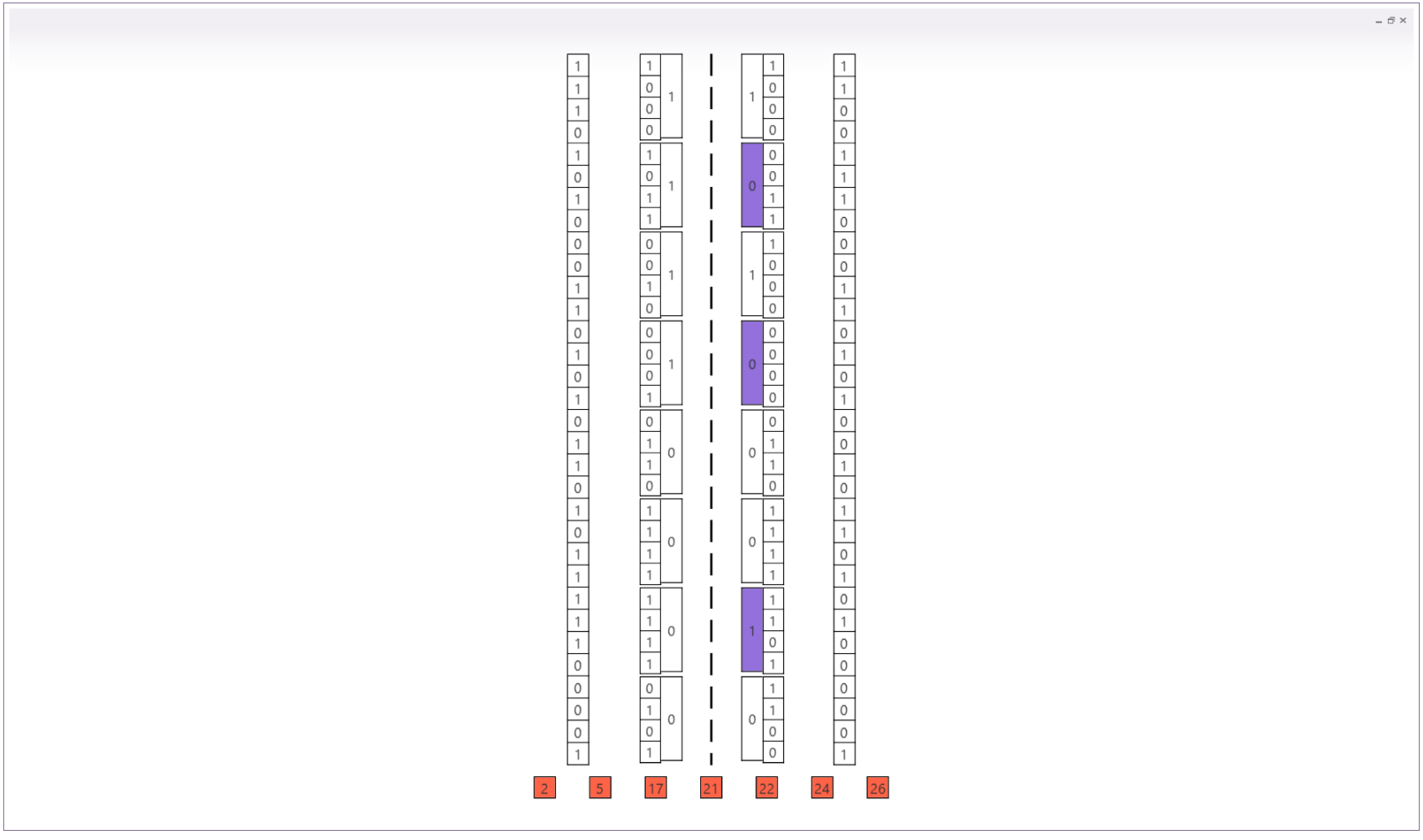
Каскадный метод коррекции ошибок



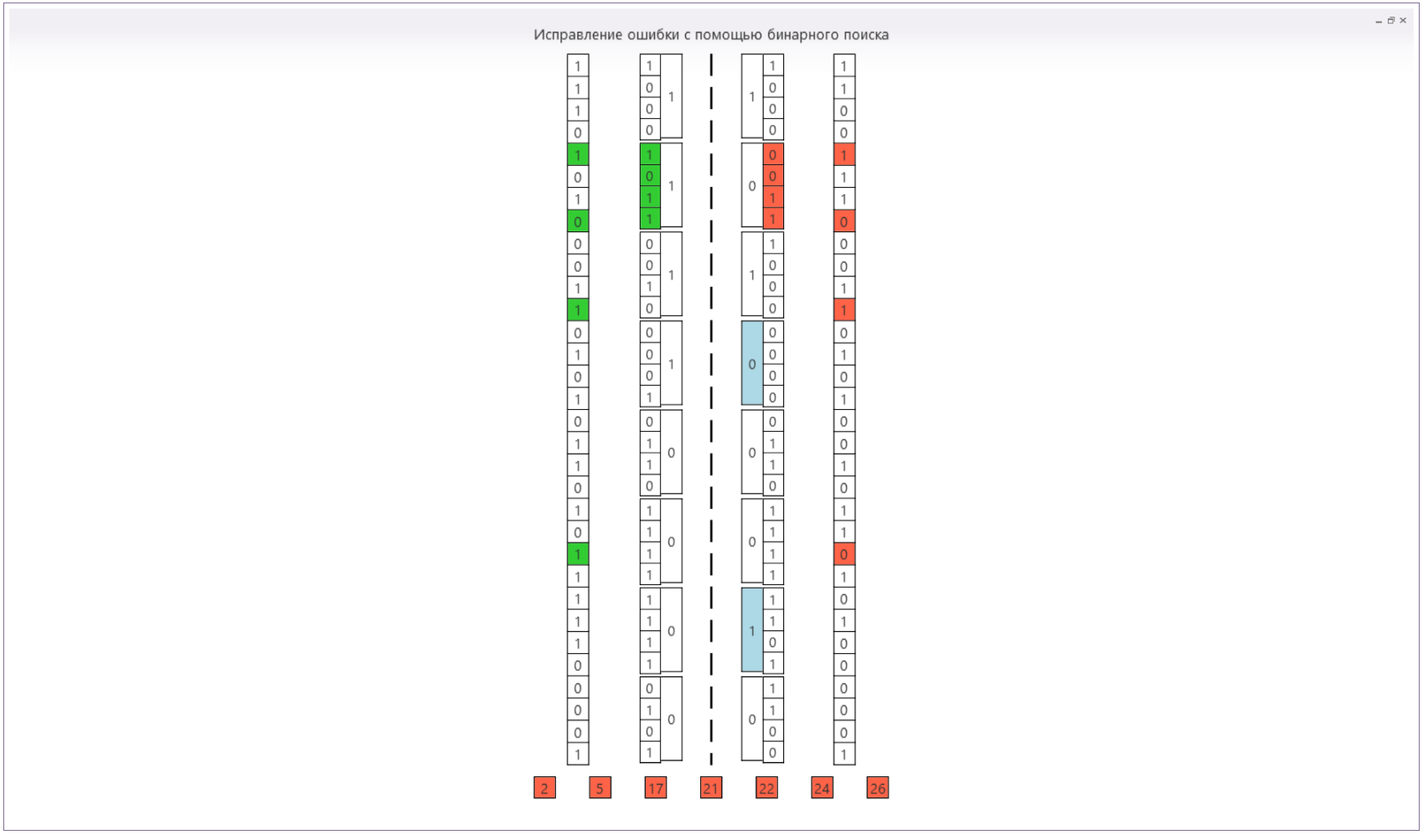
Каскадный метод коррекции ошибок



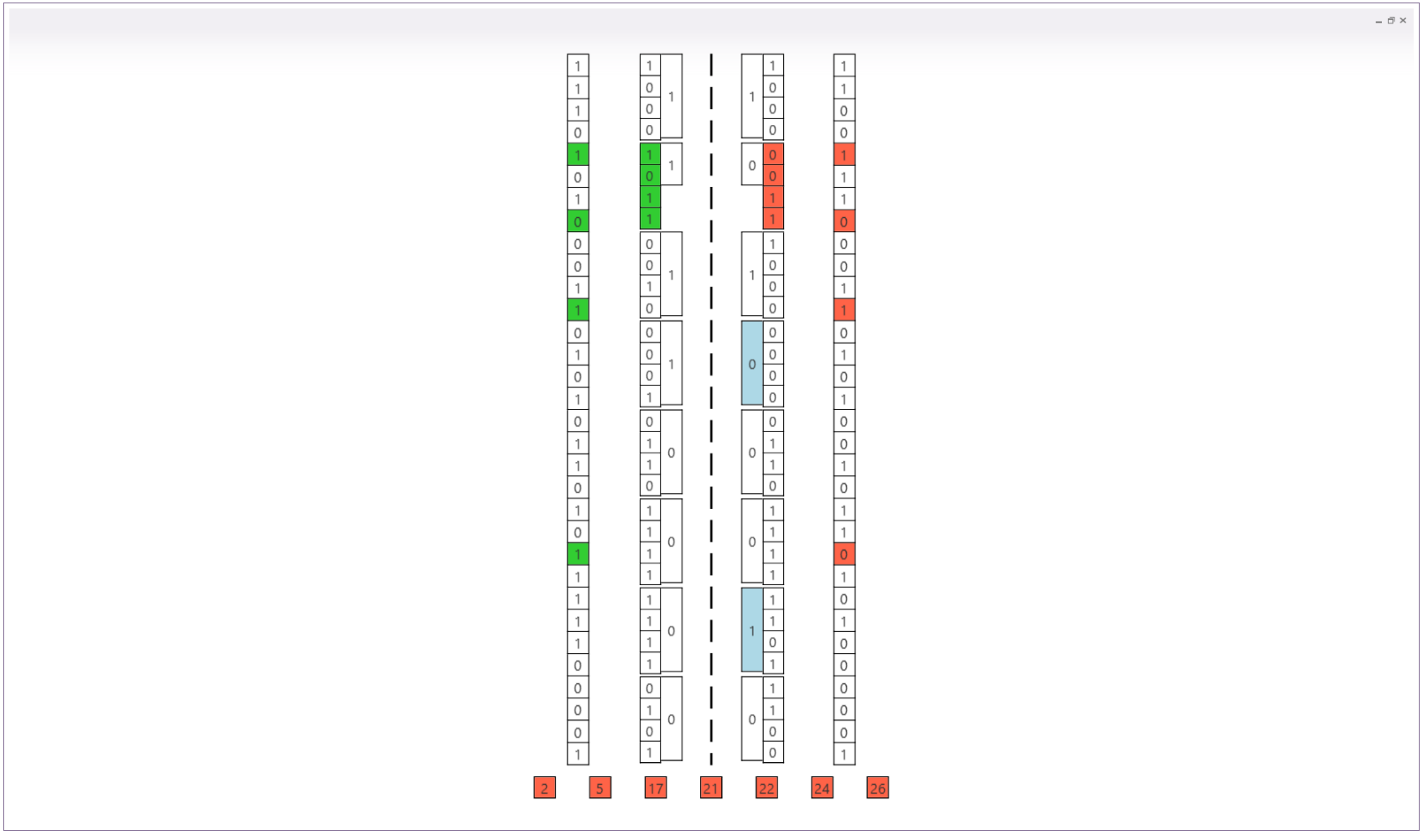
Каскадный метод коррекции ошибок



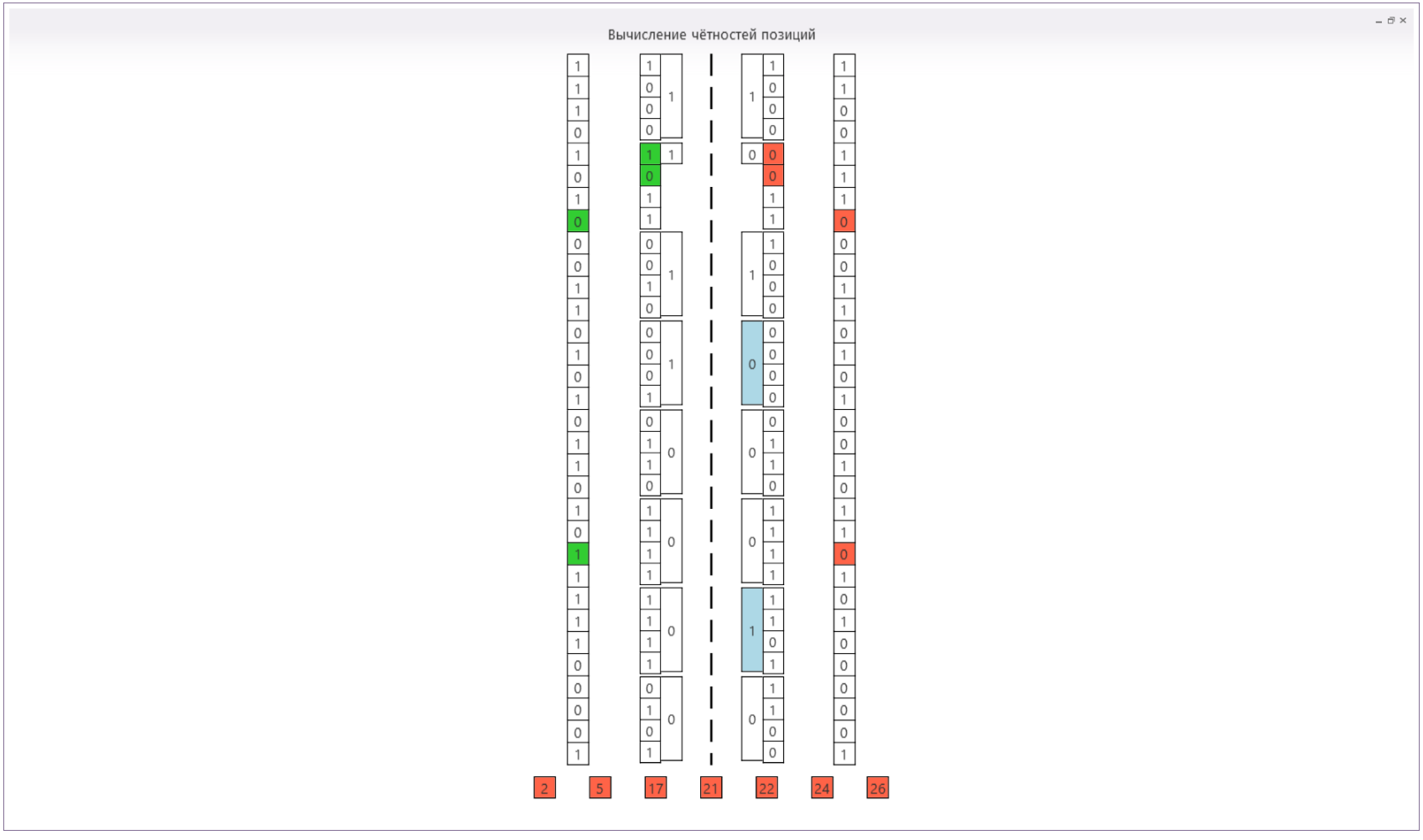
Каскадный метод коррекции ошибок



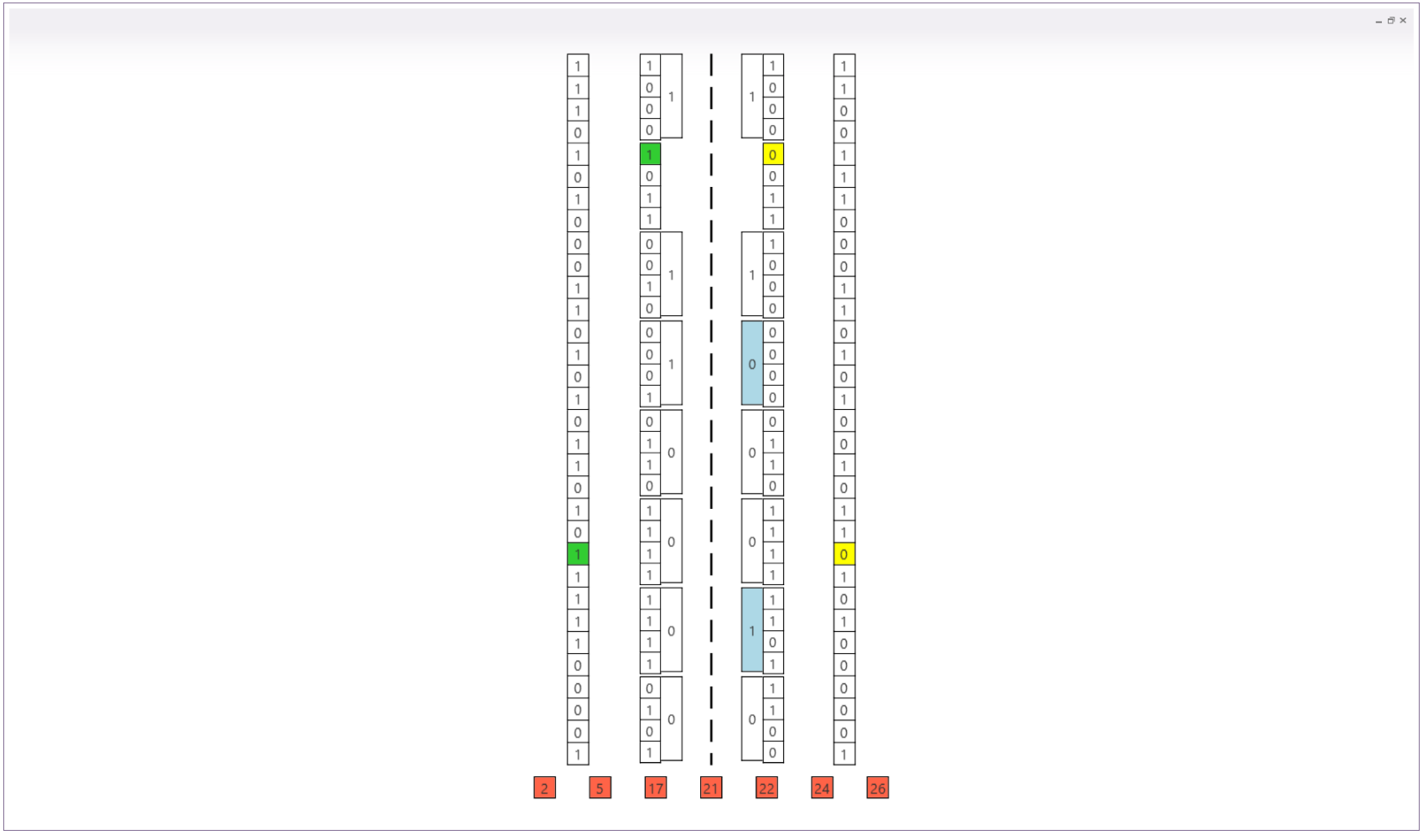
Каскадный метод коррекции ошибок



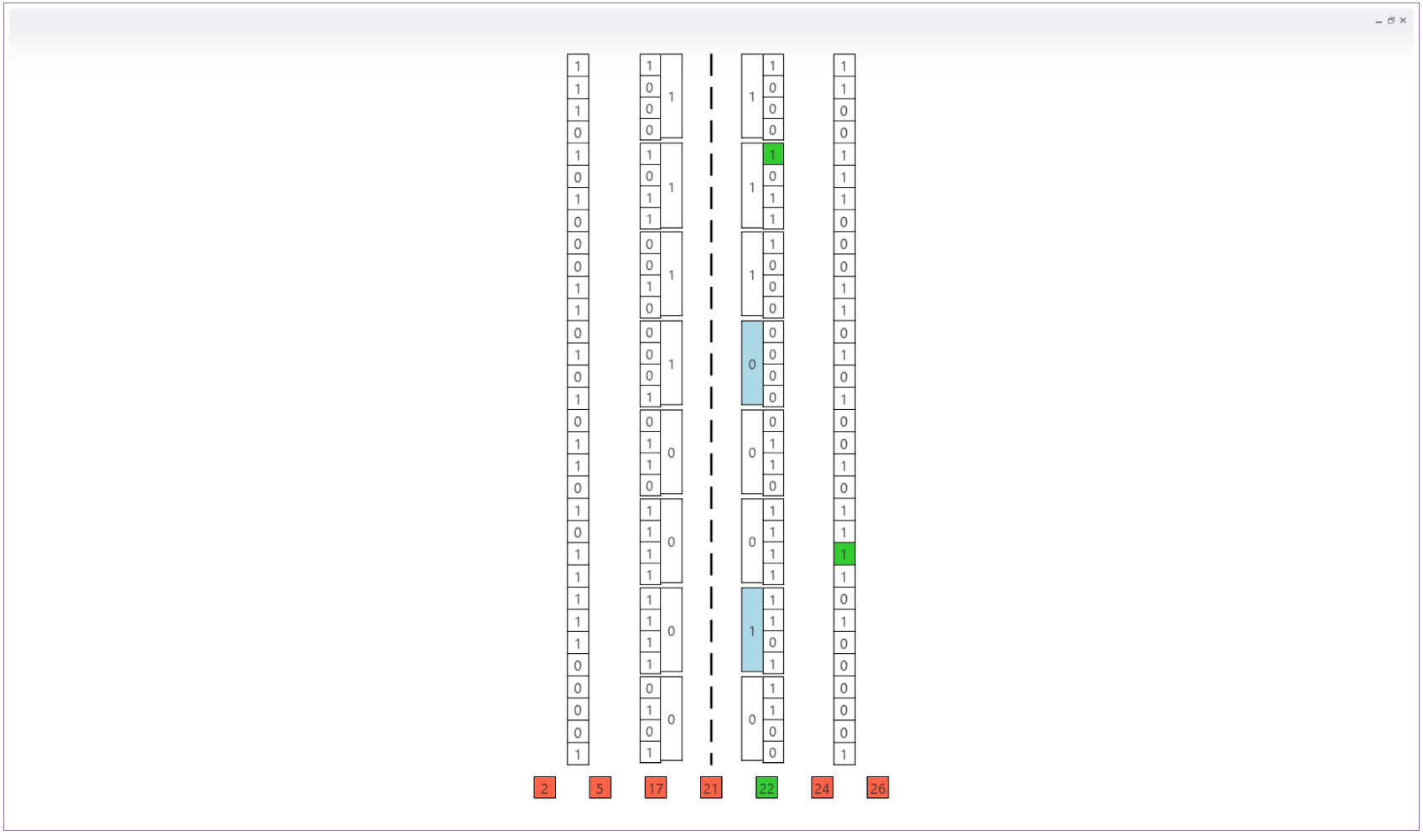
Каскадный метод коррекции ошибок



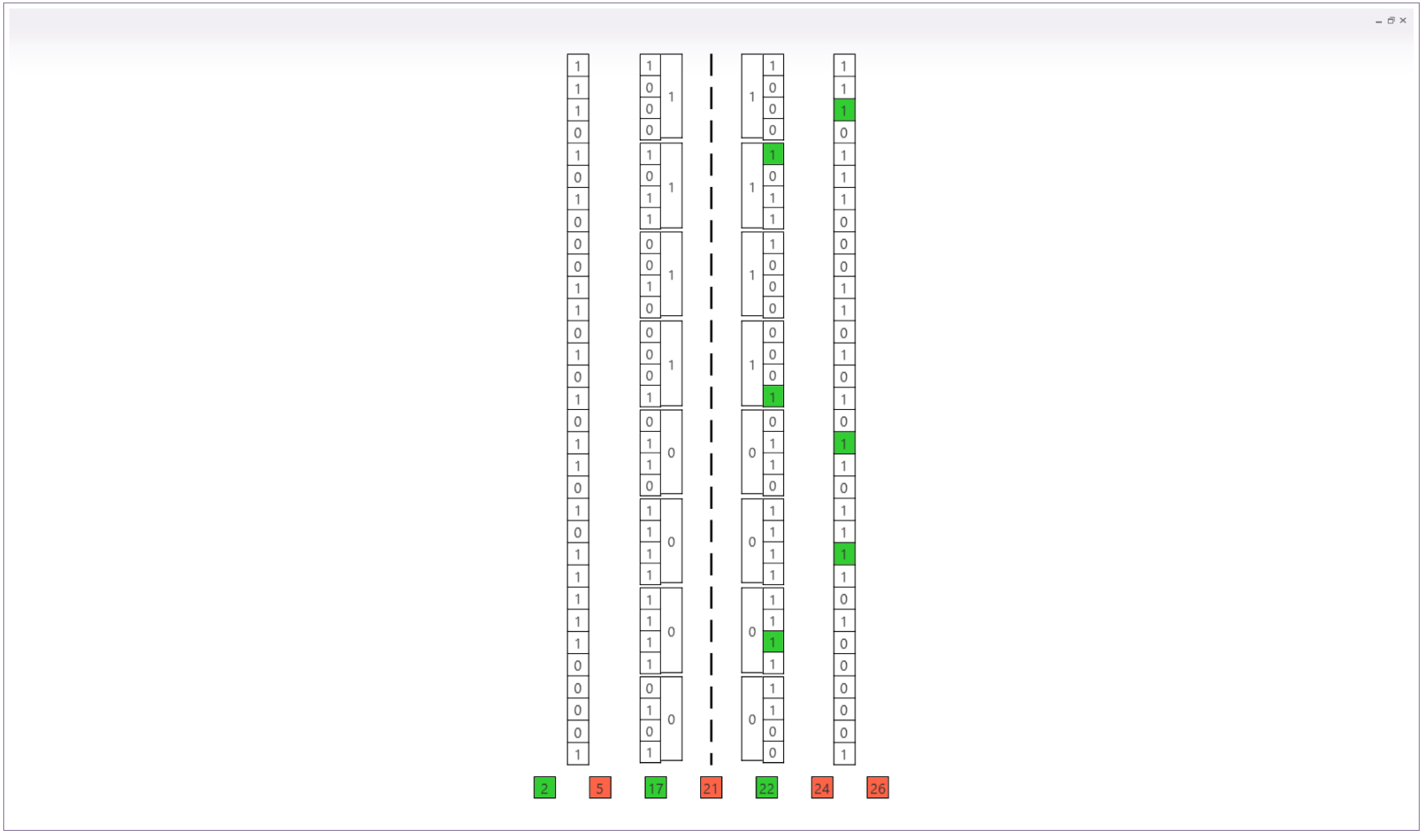
Каскадный метод коррекции ошибок



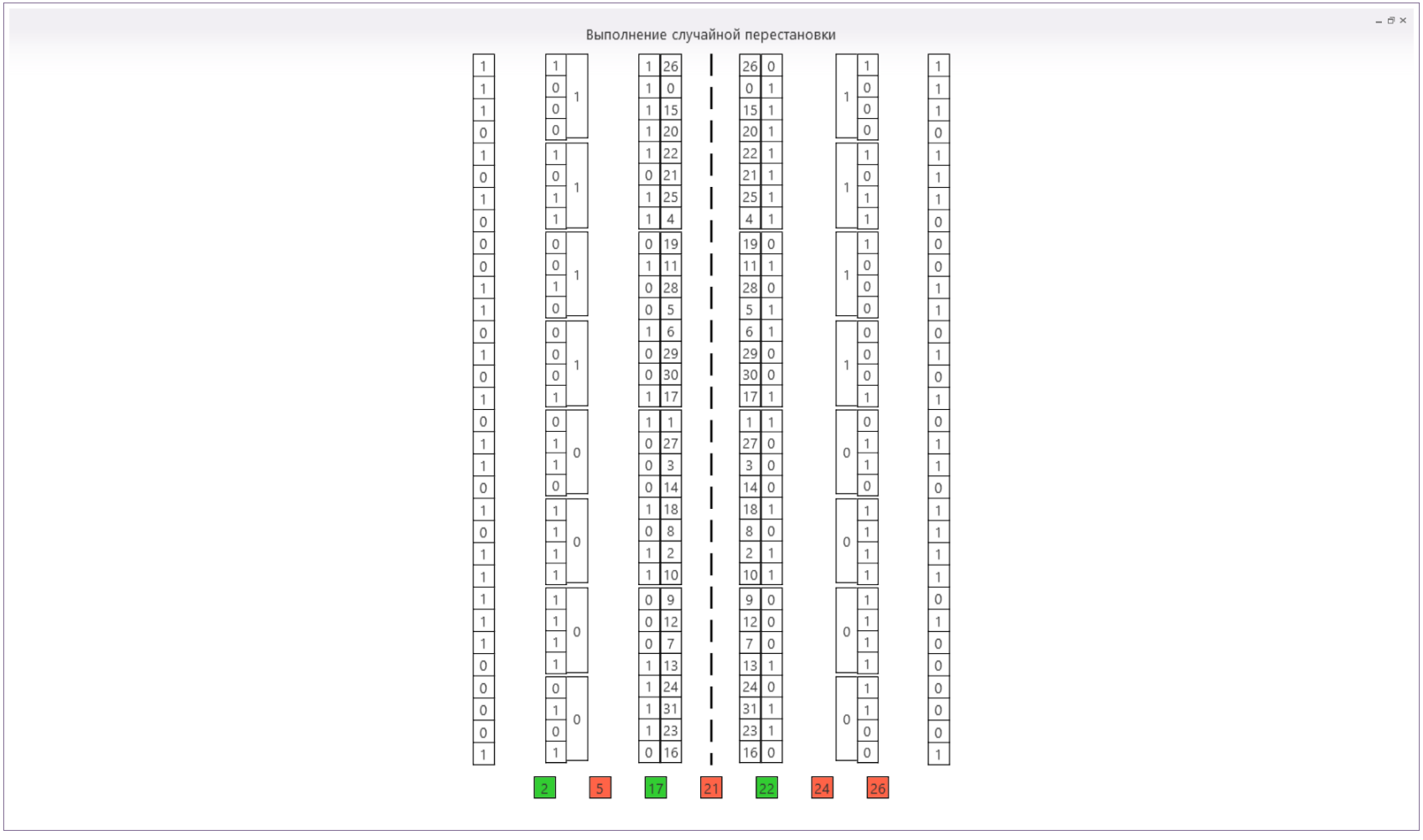
Каскадный метод коррекции ошибок



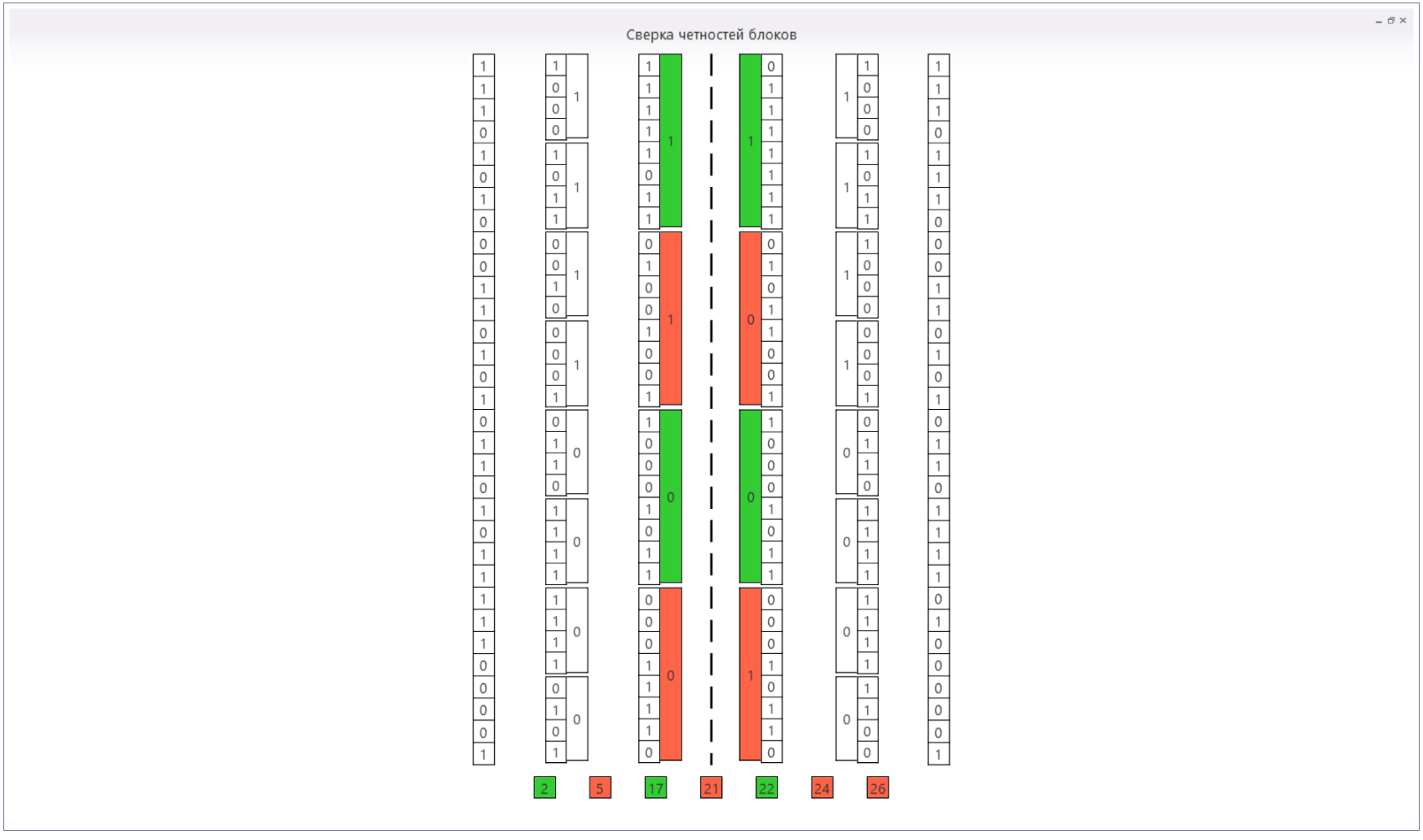
Каскадный метод коррекции ошибок



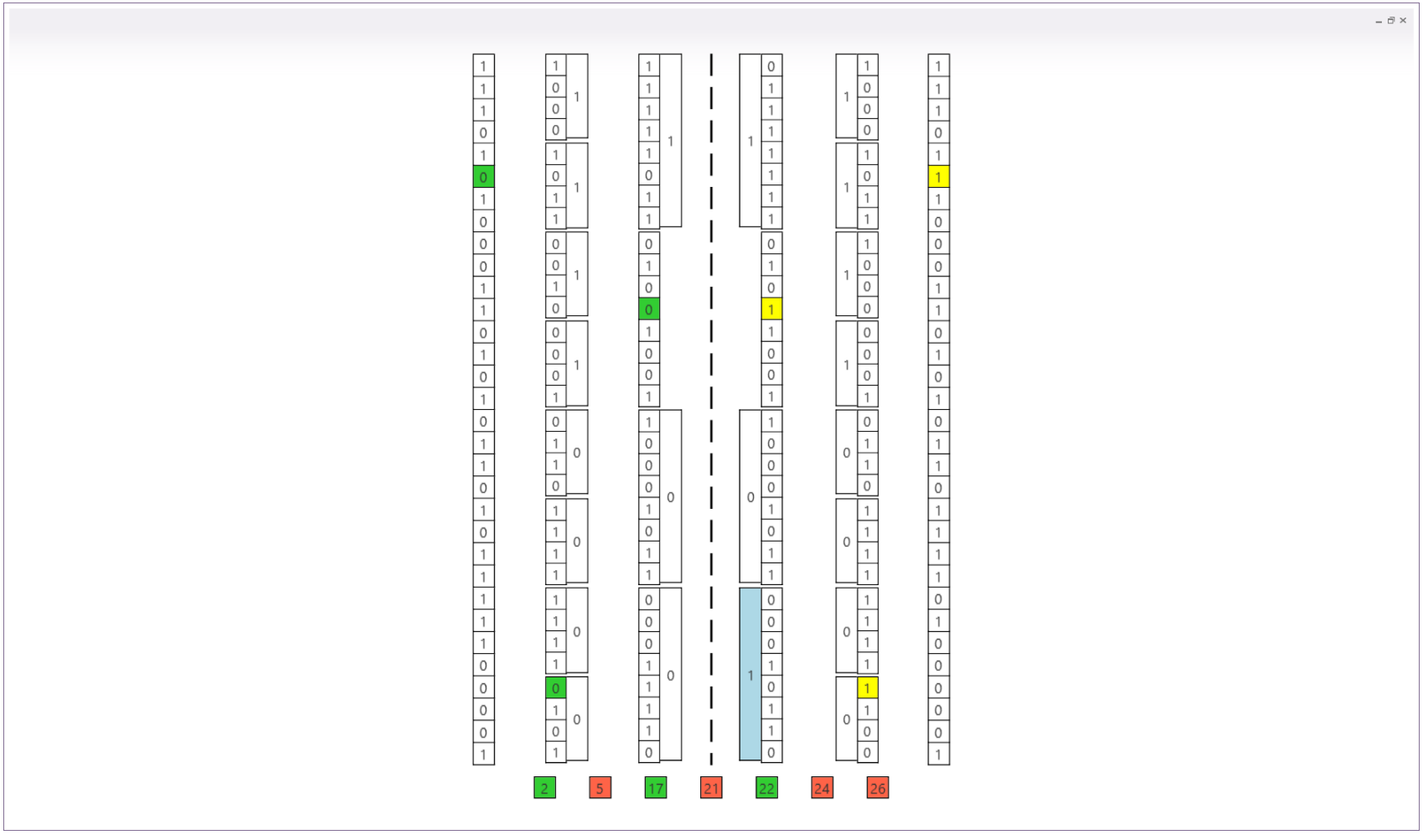
Каскадный метод коррекции ошибок



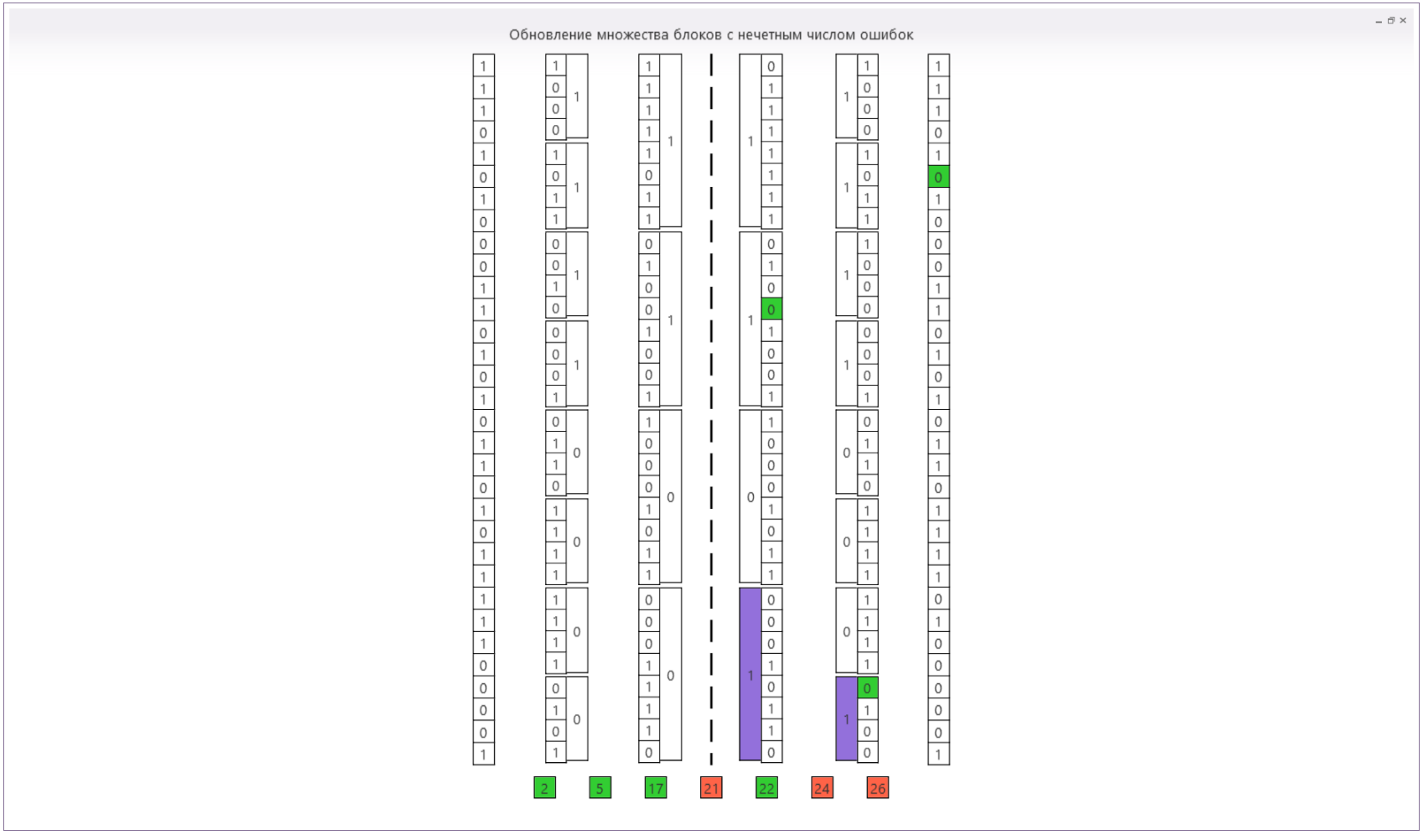
Каскадный метод коррекции ошибок



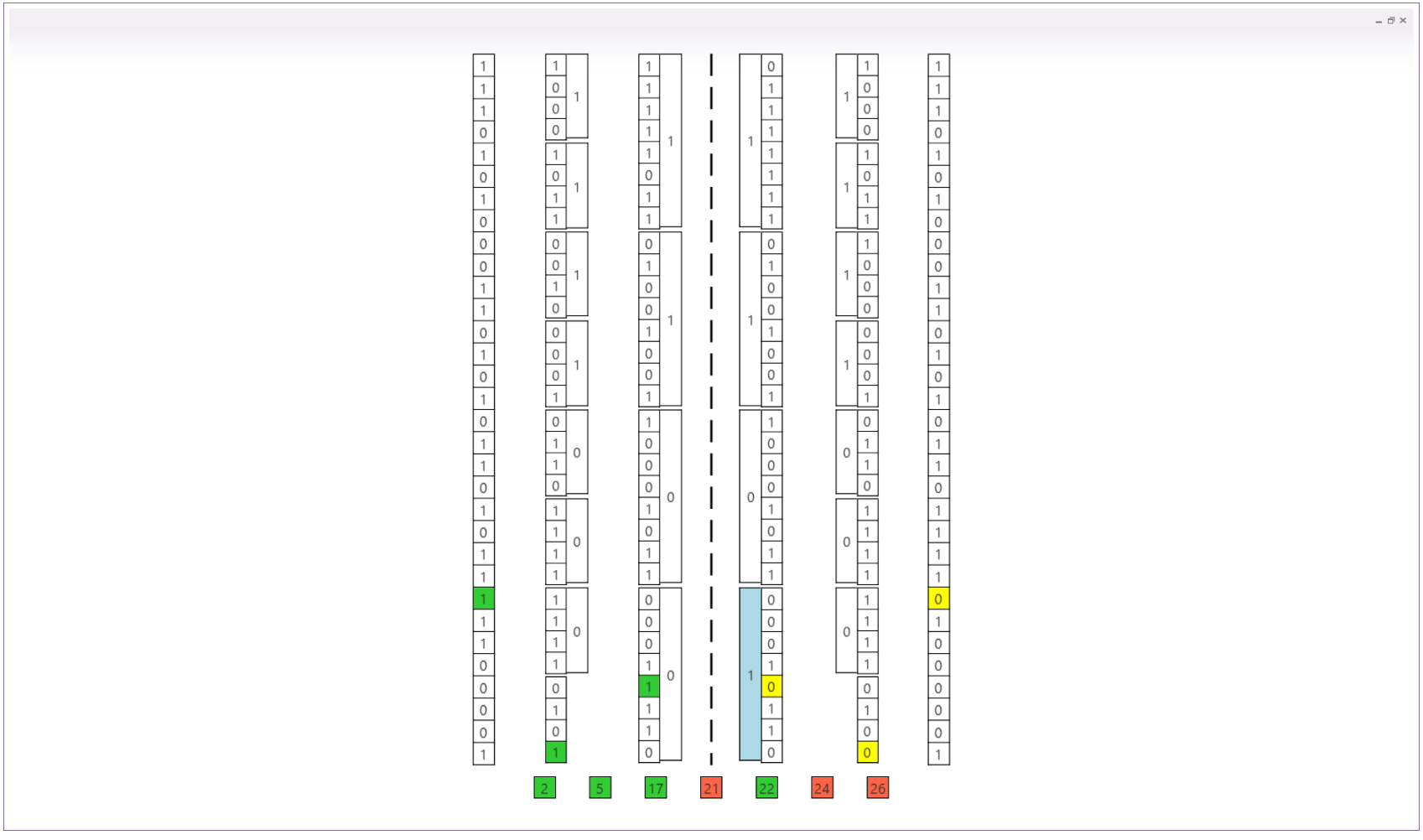
Каскадный метод коррекции ошибок



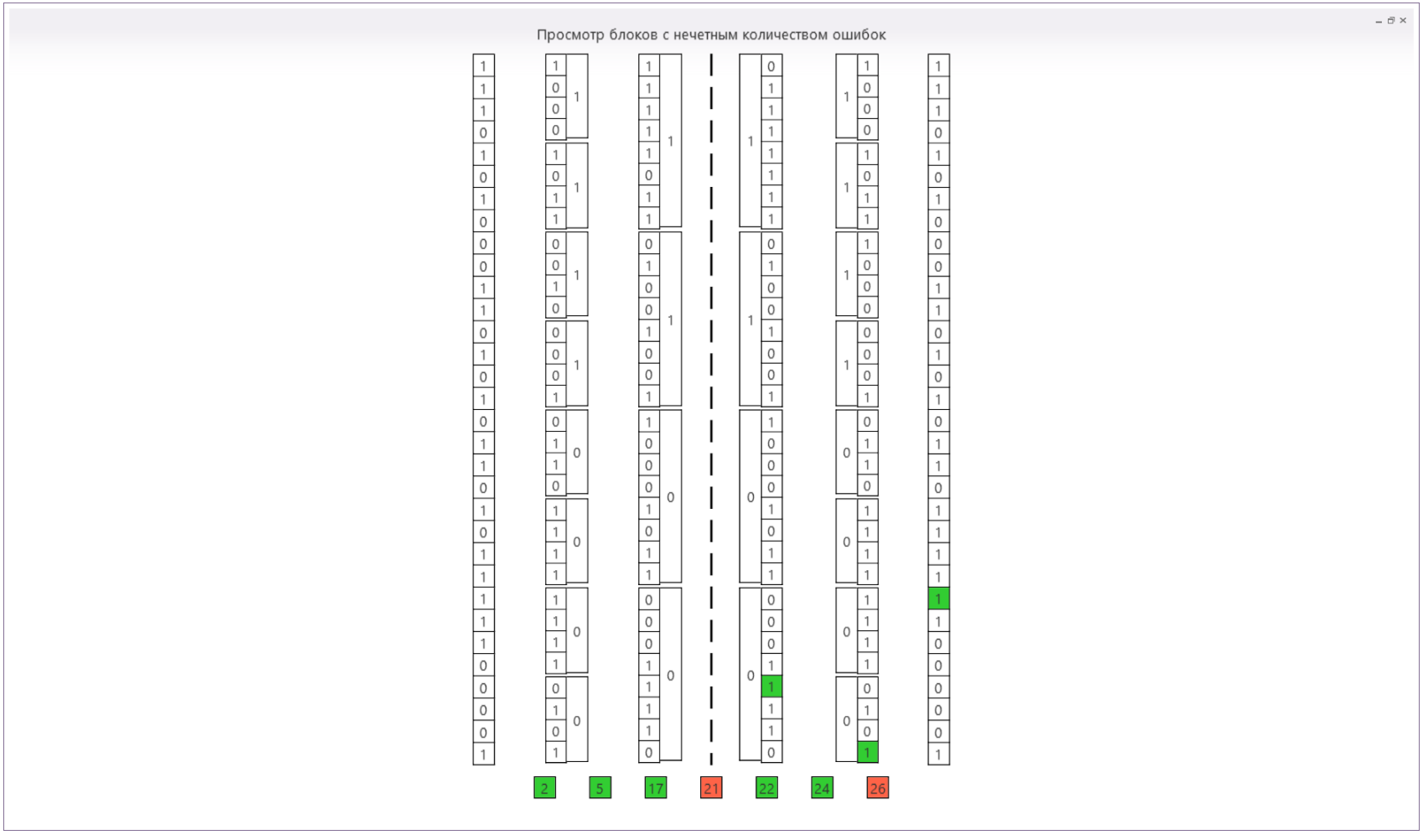
Каскадный метод коррекции ошибок



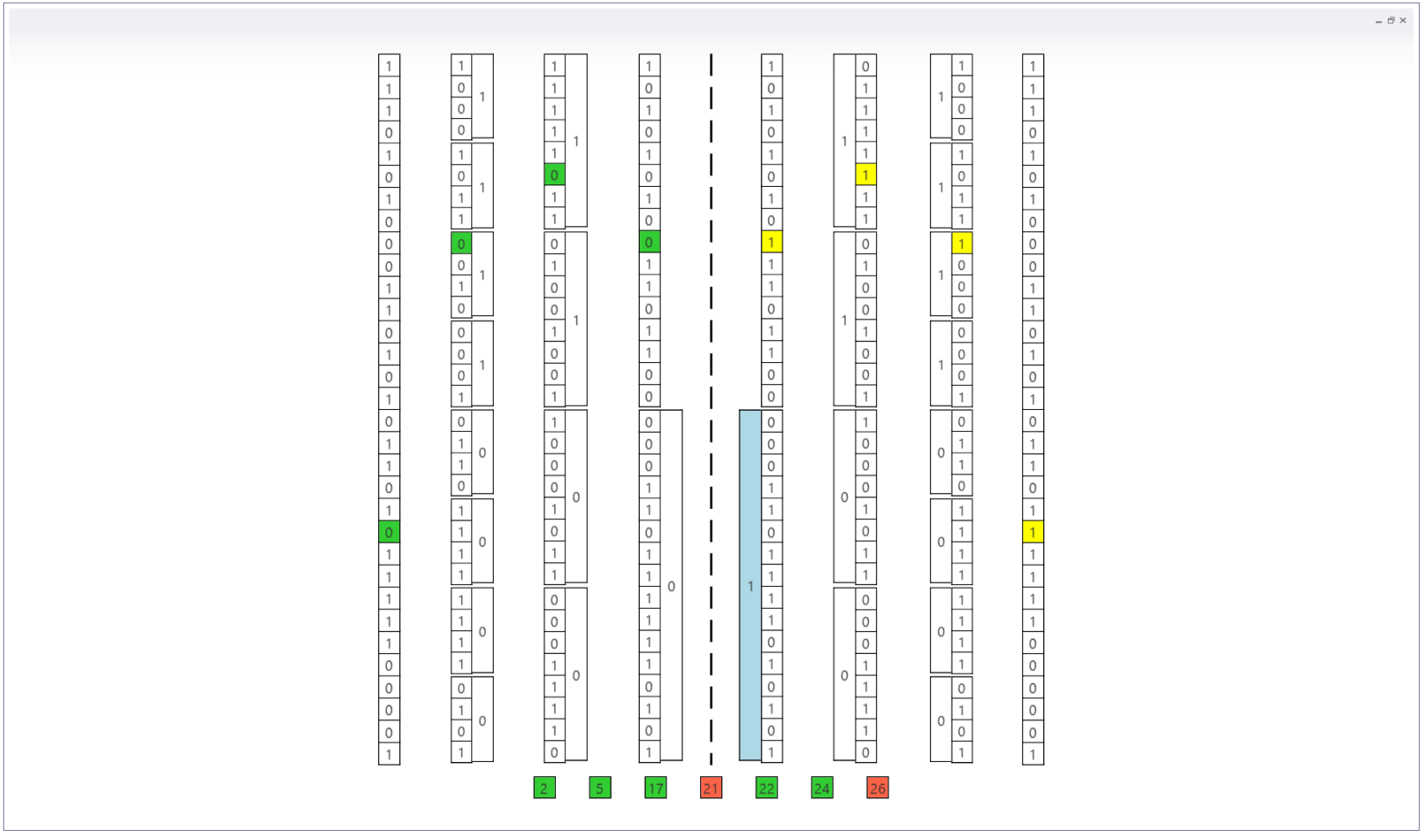
Каскадный метод коррекции ошибок



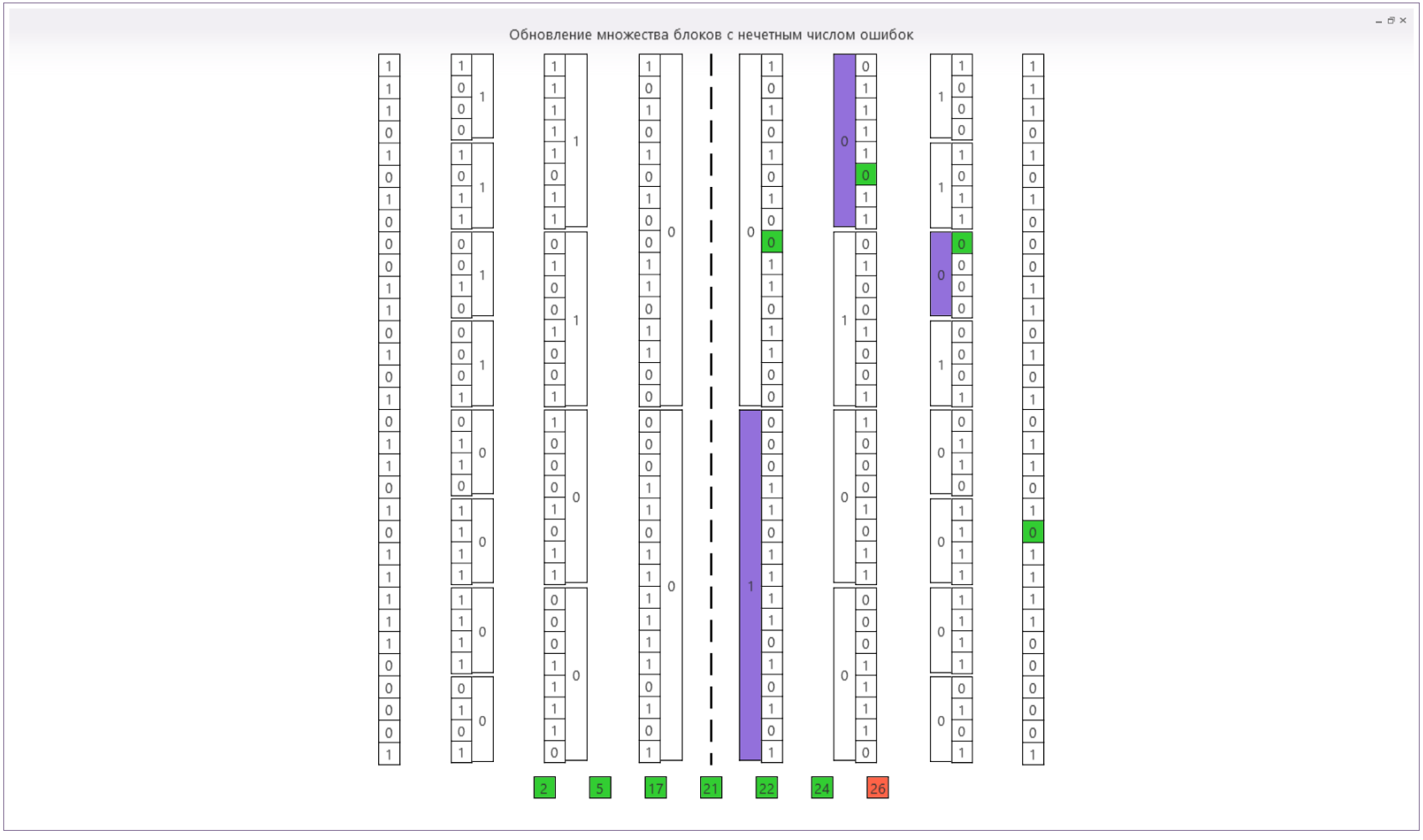
Каскадный метод коррекции ошибок



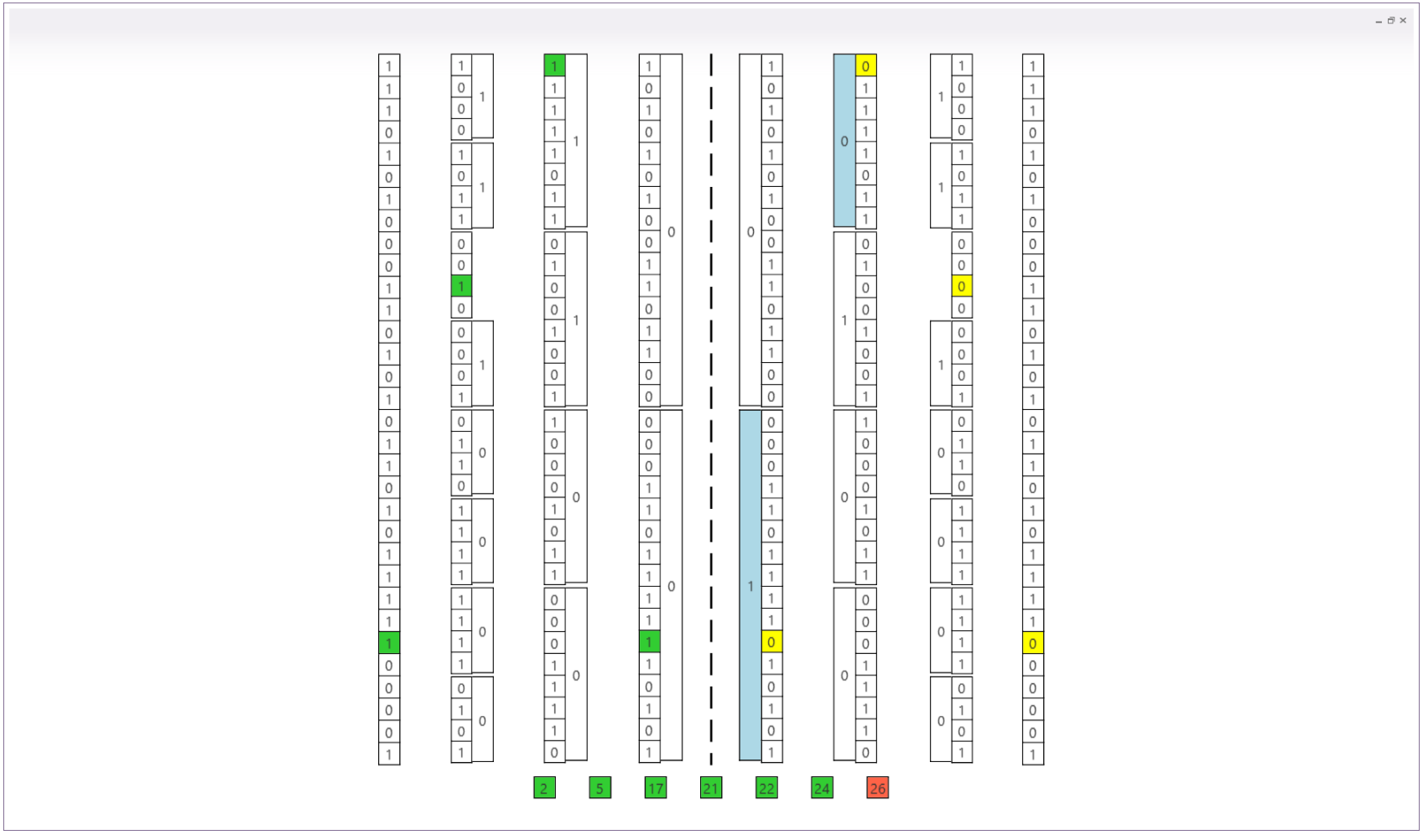
Каскадный метод коррекции ошибок



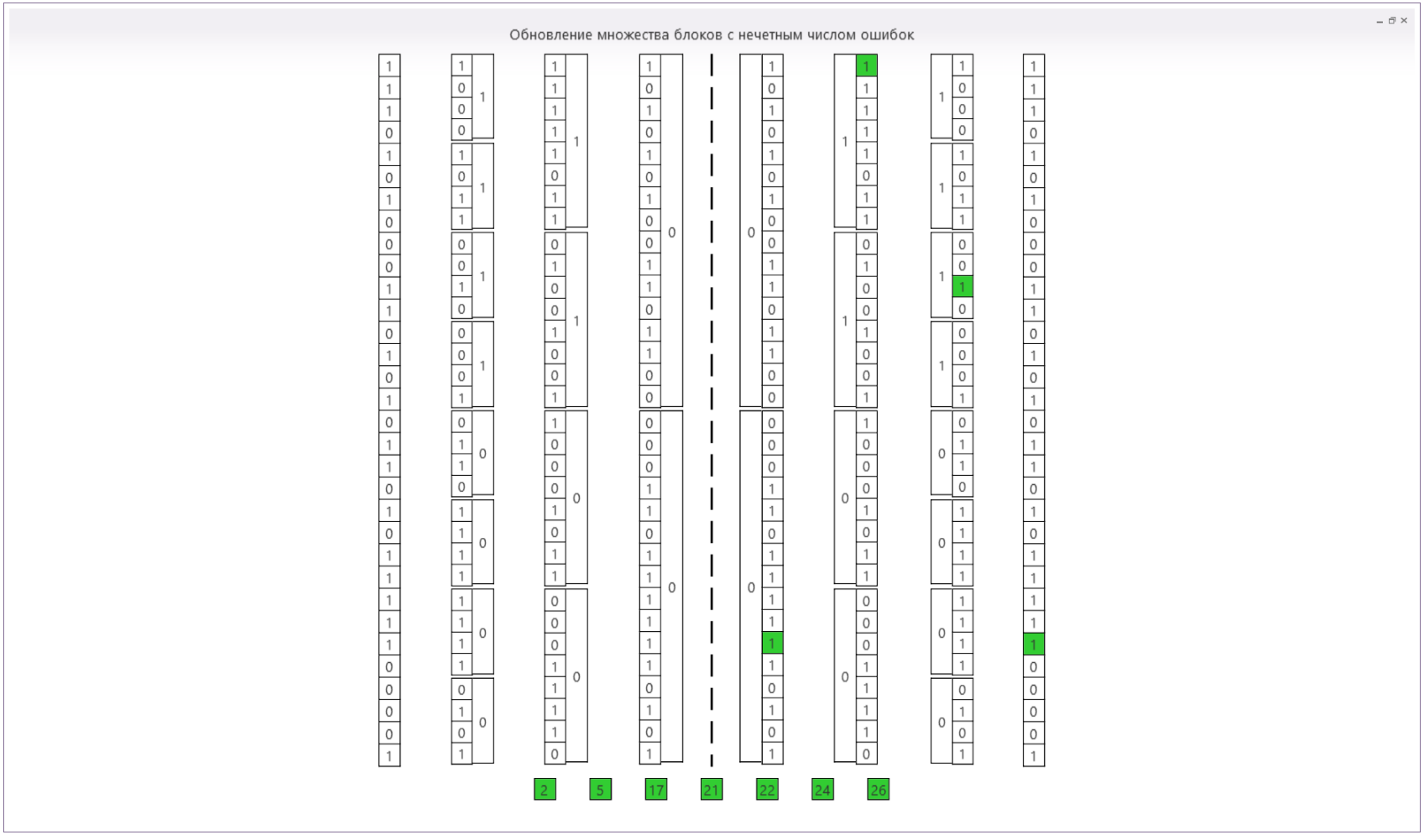
Каскадный метод коррекции ошибок



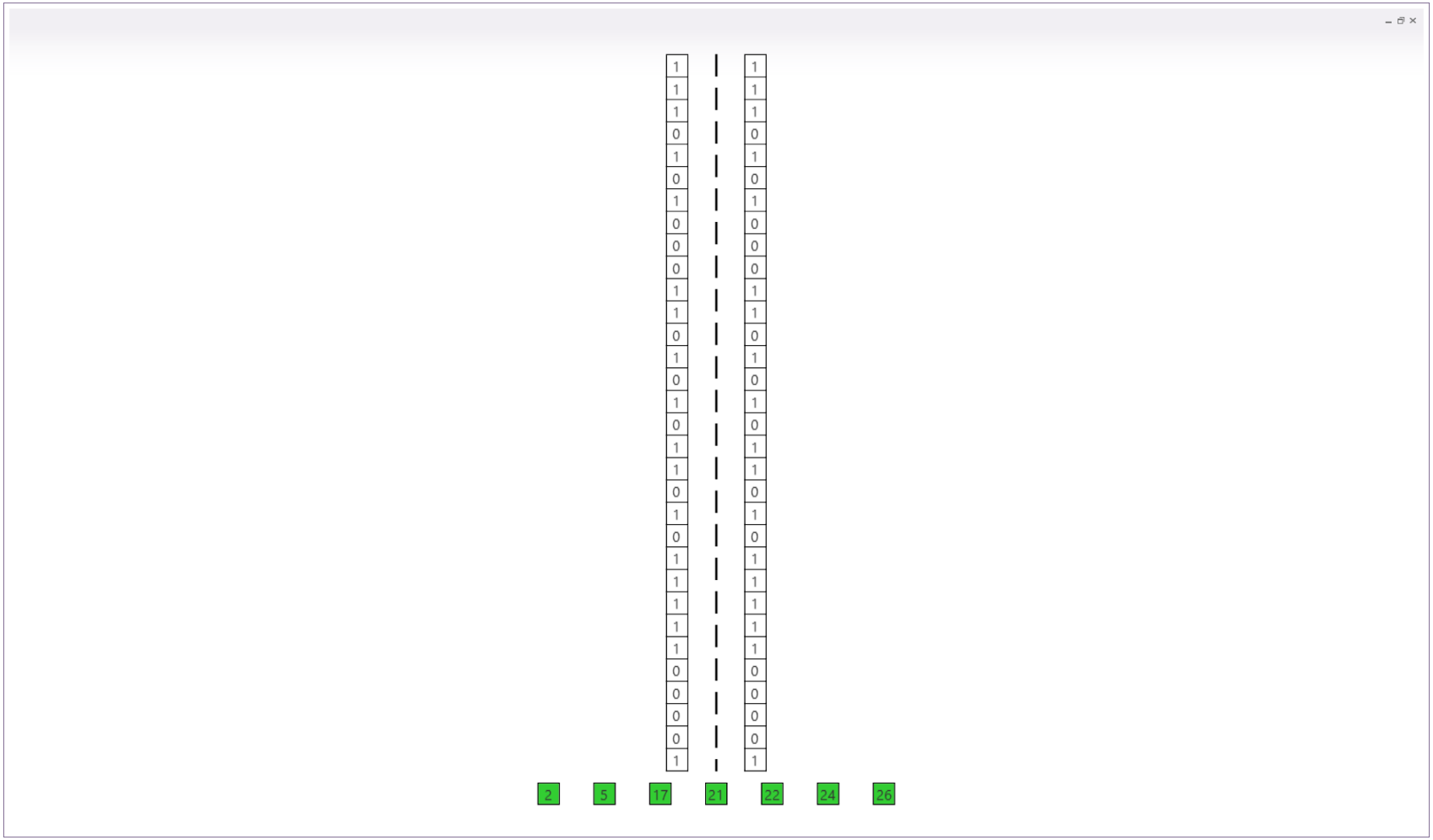
Каскадный метод коррекции ошибок



Каскадный метод коррекции ошибок



Каскадный метод коррекции ошибок



Определение

Семейство $\mathcal{F}$ функций $\mathcal{A} \to \mathcal{B}$ называется *универсальным*, если

$$[f(x_1) = f(x_2)] < \frac{1}{|\mathcal{B}|} \quad \forall x_1, x_2 \in \mathcal{A} : x_1 \neq x_2,$$

а f выбирается из $\mathcal{F}$ в соответствии с равномерным распределением.

Сжатие полученного ключа

Теорема

Пусть X — случайная величина в алфавите $\mathcal{X}$ с вероятностым распределением P_X и энтропией Реньи $R(X)$. Кроме того, пусть G — случайная величина, отвечающая случайному выбору (внутри равномерного распределения) члена универсального семейства хеш-функций, отображающих $\mathcal{X} \to \{0,1\}^r$. Тогда

$$H(G(X)|G) \geq R(G(X)|G) \geq r - \frac{2^{r-R(X)}}{\ln 2}. \qquad (1)$$

Полученные результаты

1. Показано существование и дано обоснование секретности протокола квантовой криптографии, обеспечивающего безусловную секретность в условиях потерь в линии связи и неоднофотонности источника.
2. Рассмотрен и проанализирован один из протоколов коррекции ошибок, который в настоящее время является стандартом в квантовом распределении ключей.
3. Разработаны программы, визуализирующие процессы:
   - распределения ключей по релятивистскому протоколу с имитацией атак подслушивателя и последующим детектированием возникающих из-за этого задержек,
   - коррекции ошибок по протоколу Cascade.

Моделирование релятивистской системы квантового распределения ключей

Дипломная работа

Большаков Роман Алексеевич
Научный руководитель: профессор,
д.ф-м.н. Молотков С.Н.

Московский государственный университет имени М.В. Ломоносова
Факультет вычислительной математики и кибернетики
Кафедра суперкомпьютеров и квантовой информатики

Москва, 2015