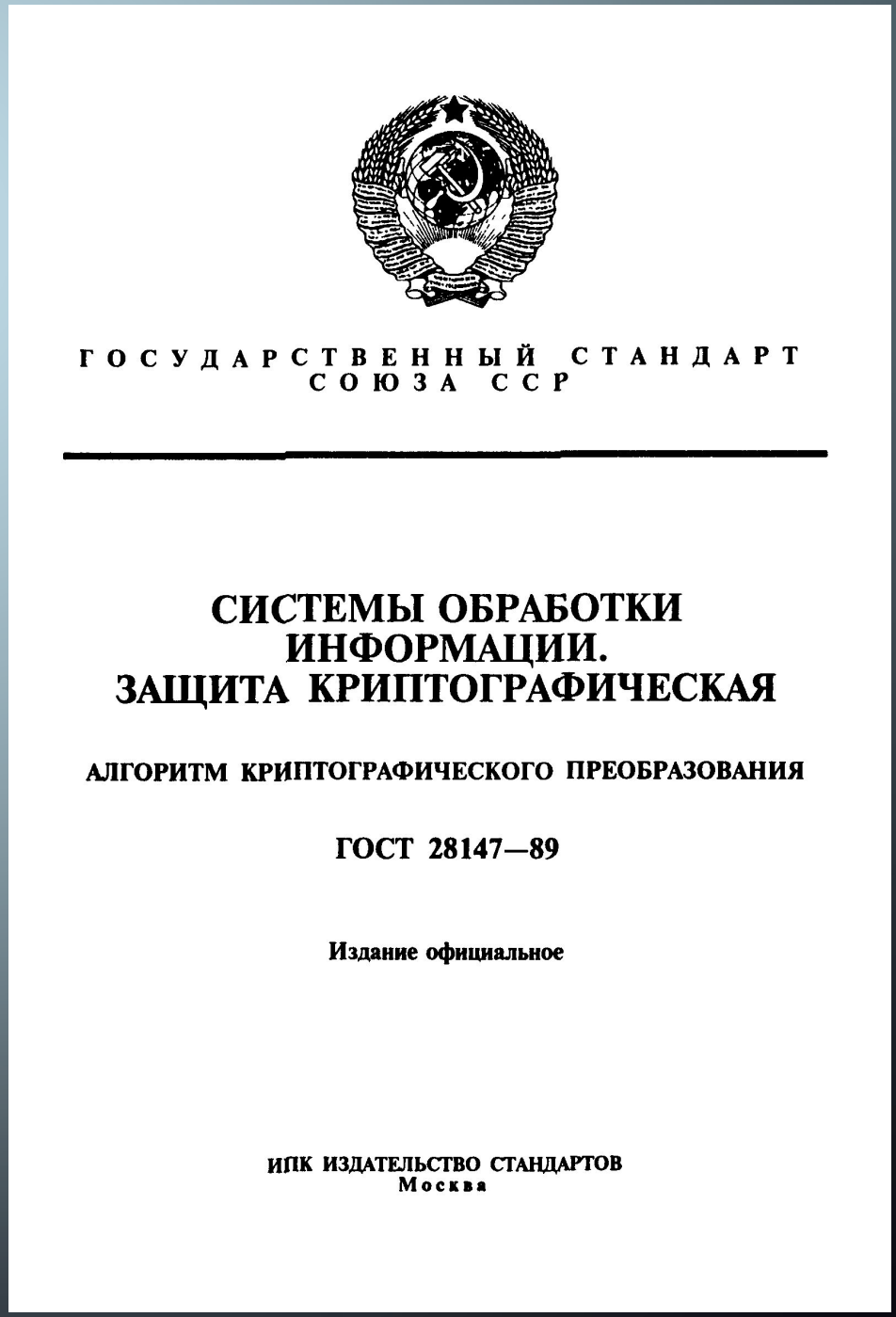
ОТЕЧЕСТВЕННЫЙ СТАНДАРТ ШИФРОВАНИЯ ГОСТ Р 34.12-15 И ЕГО СРАВНЕНИЕ СО СТАНДАРТОМ ГОСТ 28147-89

ВЫПОЛНИЛ:
СТУДЕНТ ГРУППЫ АСИ 15-1
ШКАПОВ Д.А.

МАГМА

- ГОСТ 28147-89 (Магма) — российский стандарт симметричного блочного шифрования, принятый в 1989 году. Полное название — «ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».



ГОСУДАРСТВЕННЫЙ СТАНДАРТ
СОЮЗА ССР

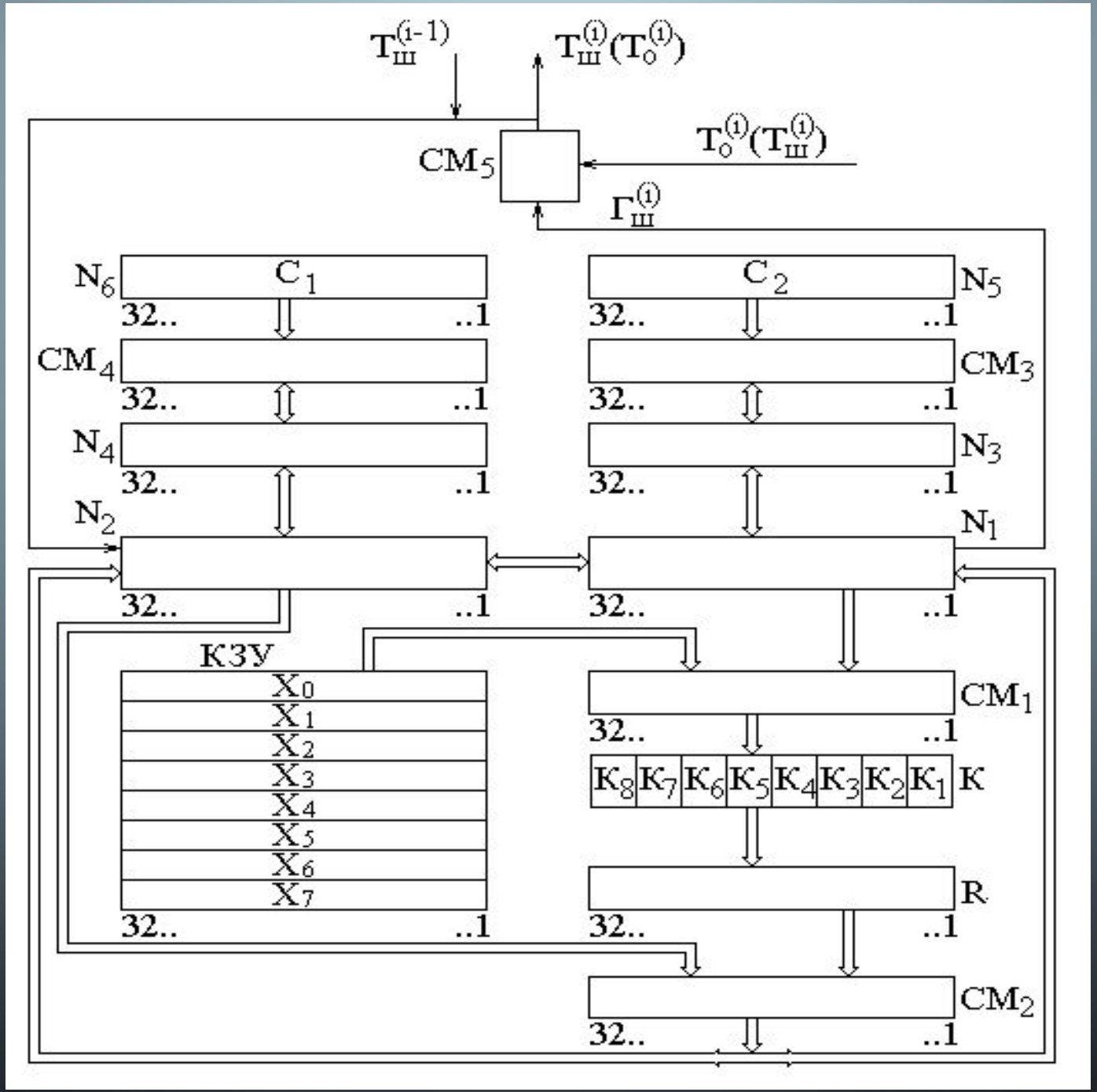
СИСТЕМЫ ОБРАБОТКИ
ИНФОРМАЦИИ.
ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ

АЛГОРИТМ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

ГОСТ 28147—89

Издание официальное

ИПК ИЗДАТЕЛЬСТВО СТАНДАРТОВ
Москва


$T_ш^{(i-1)}$
$T_ш^{(i)}(T_o^{(i)})$
CM_5
$T_o^{(i)}(T_ш^{(i)})$
$Г_ш^{(i)}$
N_6
C_1
C_2
N_5
32..
..1
CM_4
CM_3
N_4
N_3
N_2
N_1
КЗУ
X_0
X_1
X_2
X_3
X_4
X_5
X_6
X_7
CM_1
K_8 K_7 K_6 K_5 K_4 K_3 K_2 K_1 K
R
CM_2

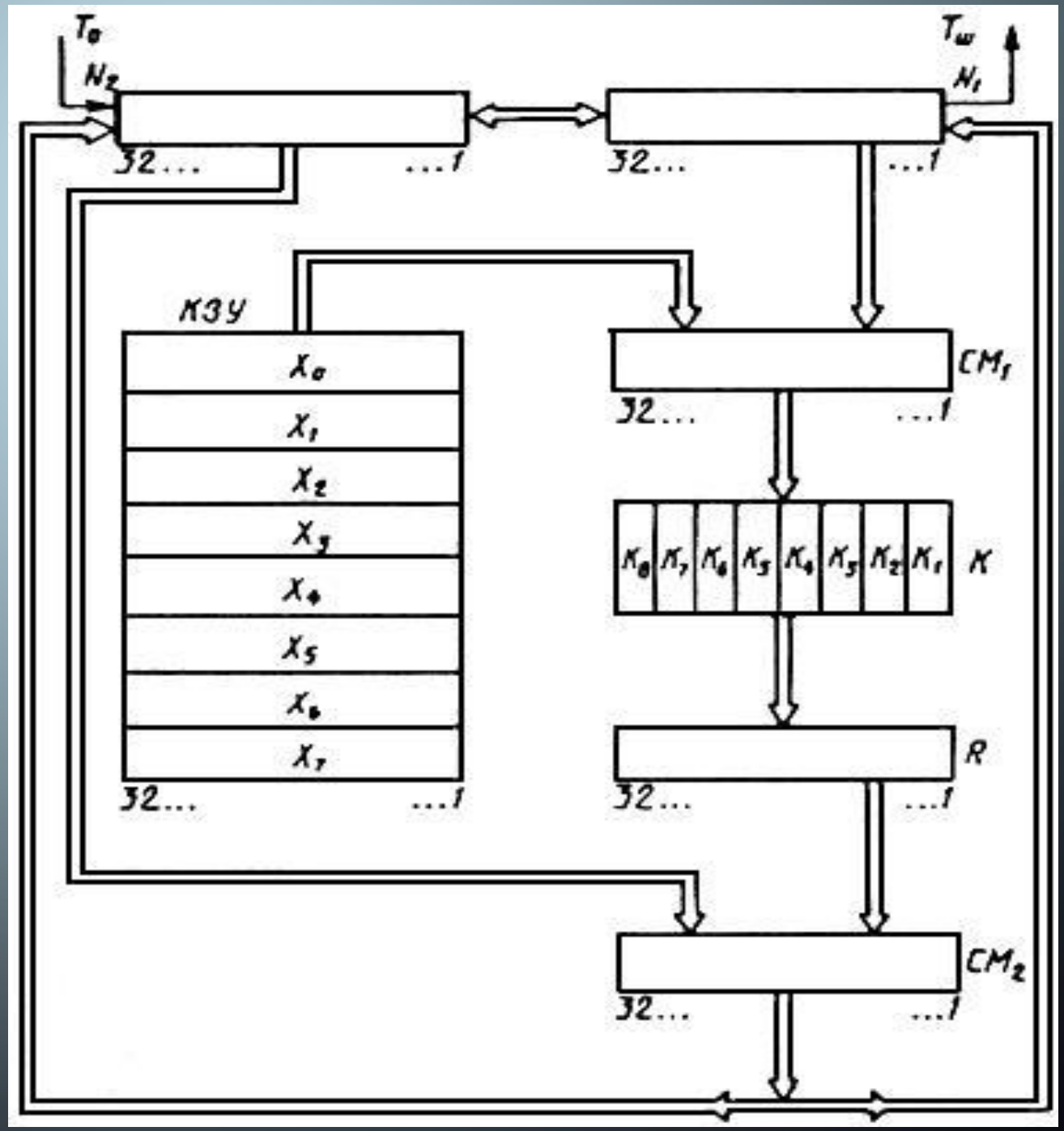
В КРИПТОСХЕМЕ ПРЕДУСМОТРЕНЫ ЧЕТЫРЕ ВИДА РАБОТЫ:

- зашифрование (расшифрование) данных в режиме простой замены;
- зашифрование (расшифрование) данных в режиме гаммирования;
- зашифрование (расшифрование) данных в режиме гаммирования с обратной связью;
- режим выработки имитовставки.

РЕЖИМ ПРОСТОЙ ЗАМЕНЫ

$$A_{i+1} = B_i \oplus f(A_i, I$$
$$B_{i+1} = A_i$$

Узел *S-блока*:
1, 15, 13, 0, 5, 7, 10, 4, 9, 2, 3, 14,
6, 11, 8, 12

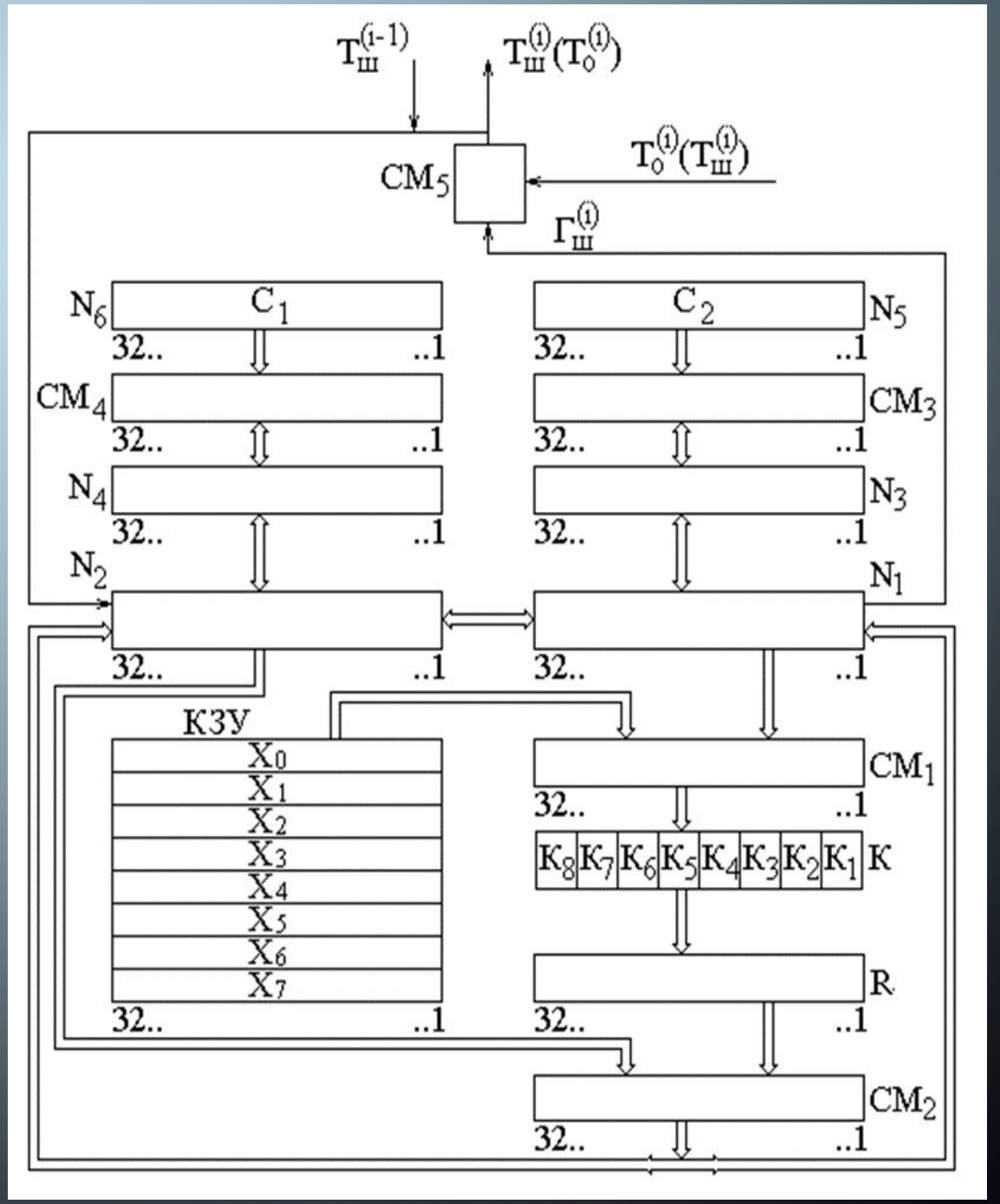


НЕДОСТАТКИ:

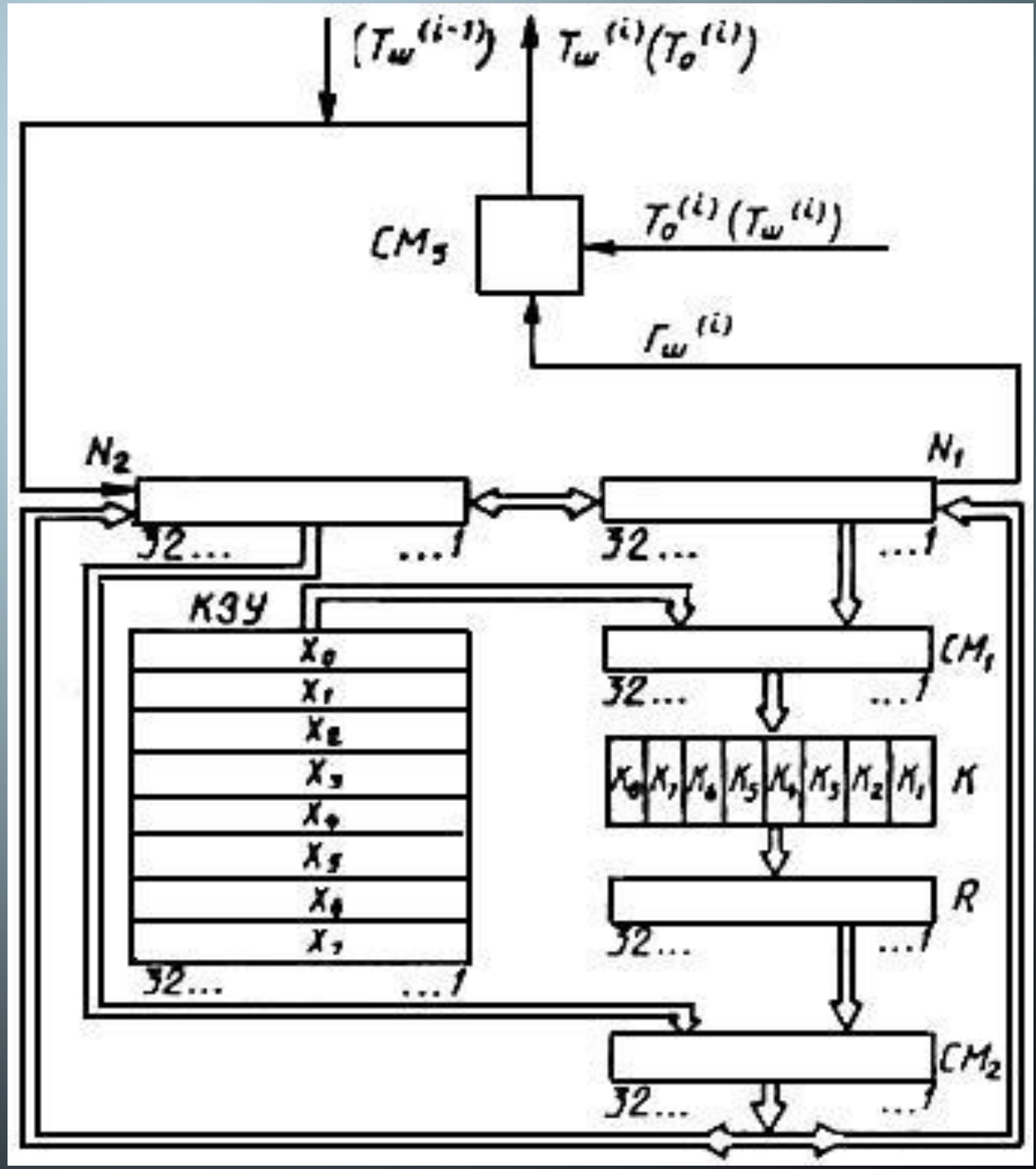
- Может применяться только для шифрования открытых текстов с длиной, кратной 64 бит
- При шифровании одинаковых блоков открытого текста получаются одинаковые блоки шифротекста, что может дать определенную информацию криптоаналитику.

РЕЖИМ ГАММИРОВАНИЯ

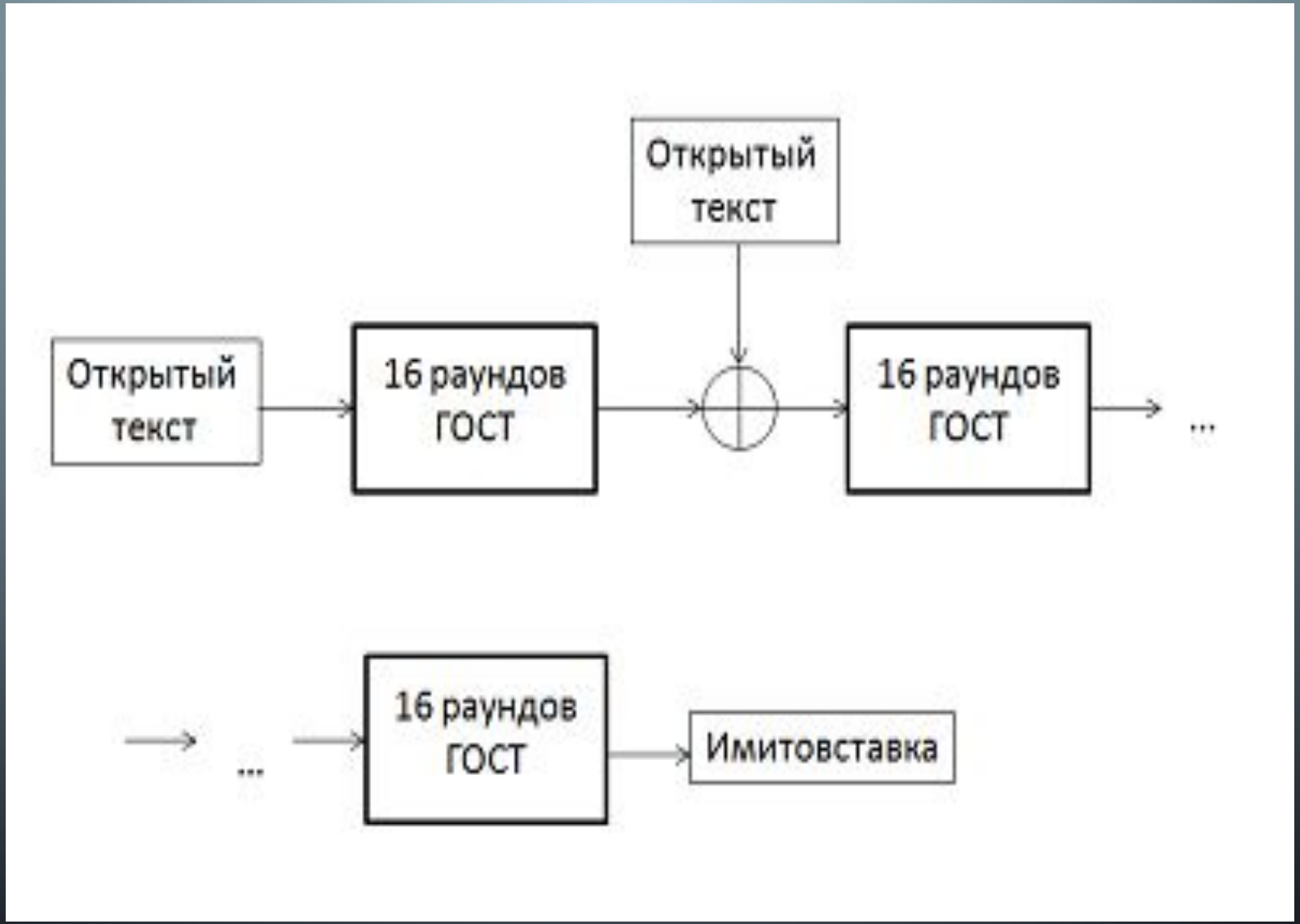
- N_3 суммируется по модулю 2^{32} с константой $C_2 = 1010101_{16}$
- N_4 суммируется по модулю 2^{32}-1 с константой $C_1 = 1010104_{16}$



РЕЖИМ ГАММИРОВАНИЯ С ОБРАТНОЙ СВЯЗЬЮ



РЕЖИМ ВЫРАБОТКИ ИМИТОВСТАВКИ

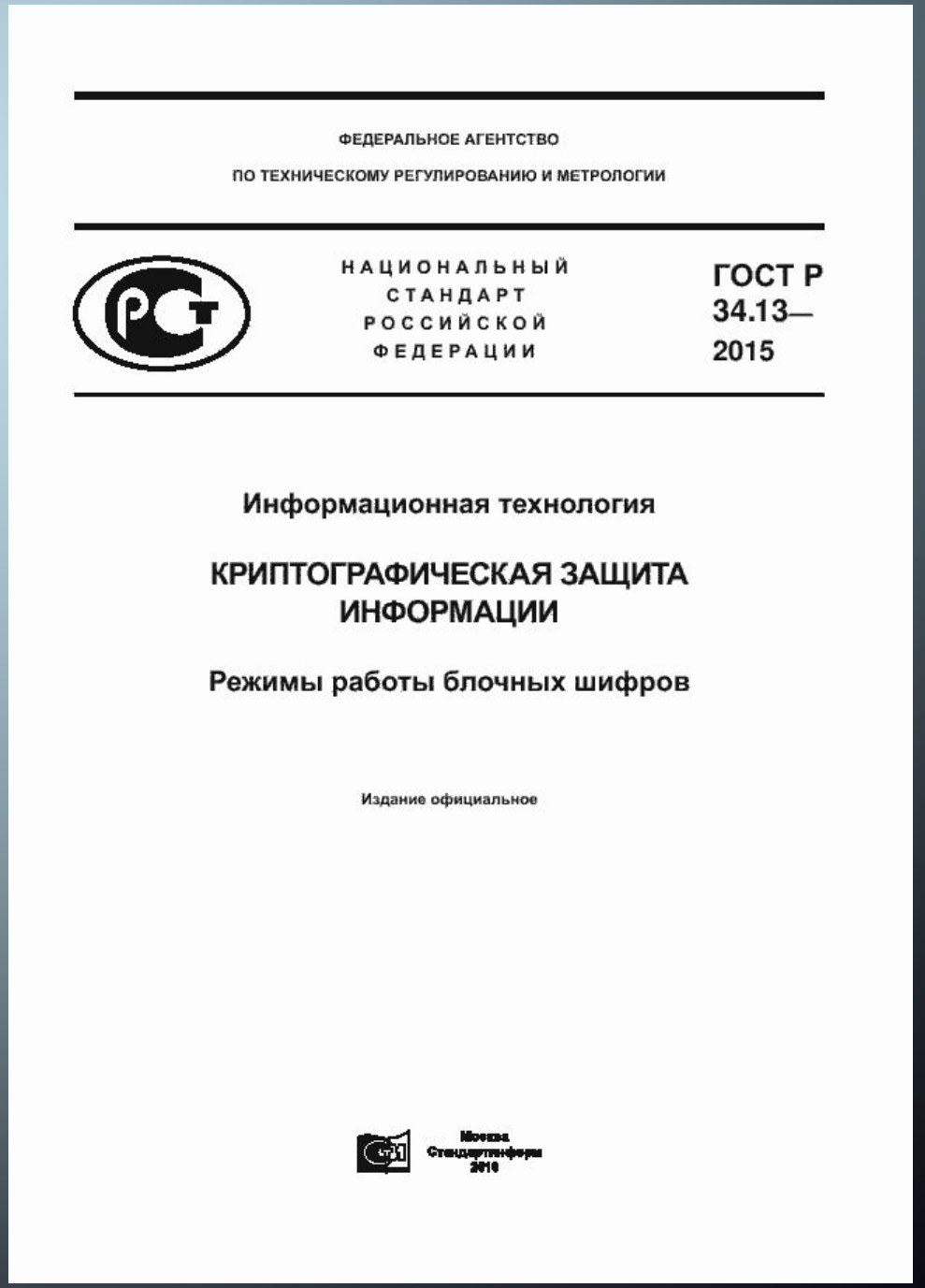


ОСНОВНЫЕ ПРОБЛЕМЫ СТАНДАРТА

- нельзя определить криптостойкость алгоритма, не зная заранее таблицы замен;
- реализации алгоритма от различных производителей могут использовать разные таблицы замен и могут быть несовместимы между собой;
- возможность преднамеренного предоставления слабых таблиц замен лицензирующими органами РФ;
- потенциальная возможность (отсутствие запрета в стандарте) использования таблиц замены, в которых узлы не являются перестановками, что может привести к чрезвычайному снижению стойкости шифра.

«КУЗНЕЧИК» И «МАГМА»

- ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры»
- В стандарт включен новый блочный шифр (шифр «Кузнечик») типа «подстановочно-перестановочная сеть» с размером блока 128 бит.
- В стандарт также включено



ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 34.13— 2015

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Режимы работы блочных шифров

Издание официальное

«КУЗНЕЧИК» - АЛГОРИТМ БЛОЧНОГО ШИФРОВАНИЯ С ДЛИНОЙ БЛОКА N = 128 БИТ

128-битный входной вектор очередного раунда складывается побитно с раундовым ключом:

$$X[k]\colon V_{128} \to V_{128} \qquad X[k](a) = k \oplus a, \text{ где } k, a \in V_{128}$$

Нелинейное преобразование:

$$S\colon V_{128} \to V_{128} \qquad S(a) = S(a_{15}||\dots||a_0) = \pi(a_{15})||\dots||\pi(a_0),$$

$$\text{где } a = a_{15}||\dots||a_0 \in V_{128}, a_i \in V_8, i = 0, 1, \dots, 15;$$

Линейное преобразование:

$$R\colon V_{128} \to V_{128} \qquad R(a) = R(a_{15}||\dots||a_0) = \ell(a_{15}, \dots, a_0)||a_{15}||\dots||a_1,$$

$$\text{где } a = a_{15}||\dots||a_0 \in V_{128}, a_i \in V_8, i = 0, 1, \dots, 15;$$

$$L\colon V_{128} \to V_{128} \qquad L(a) = R^{15}(a),$$

$$\text{где } a \in V_{128}$$

РАУНДОВОЕ ПРЕОБРАЗОВАНИЕ

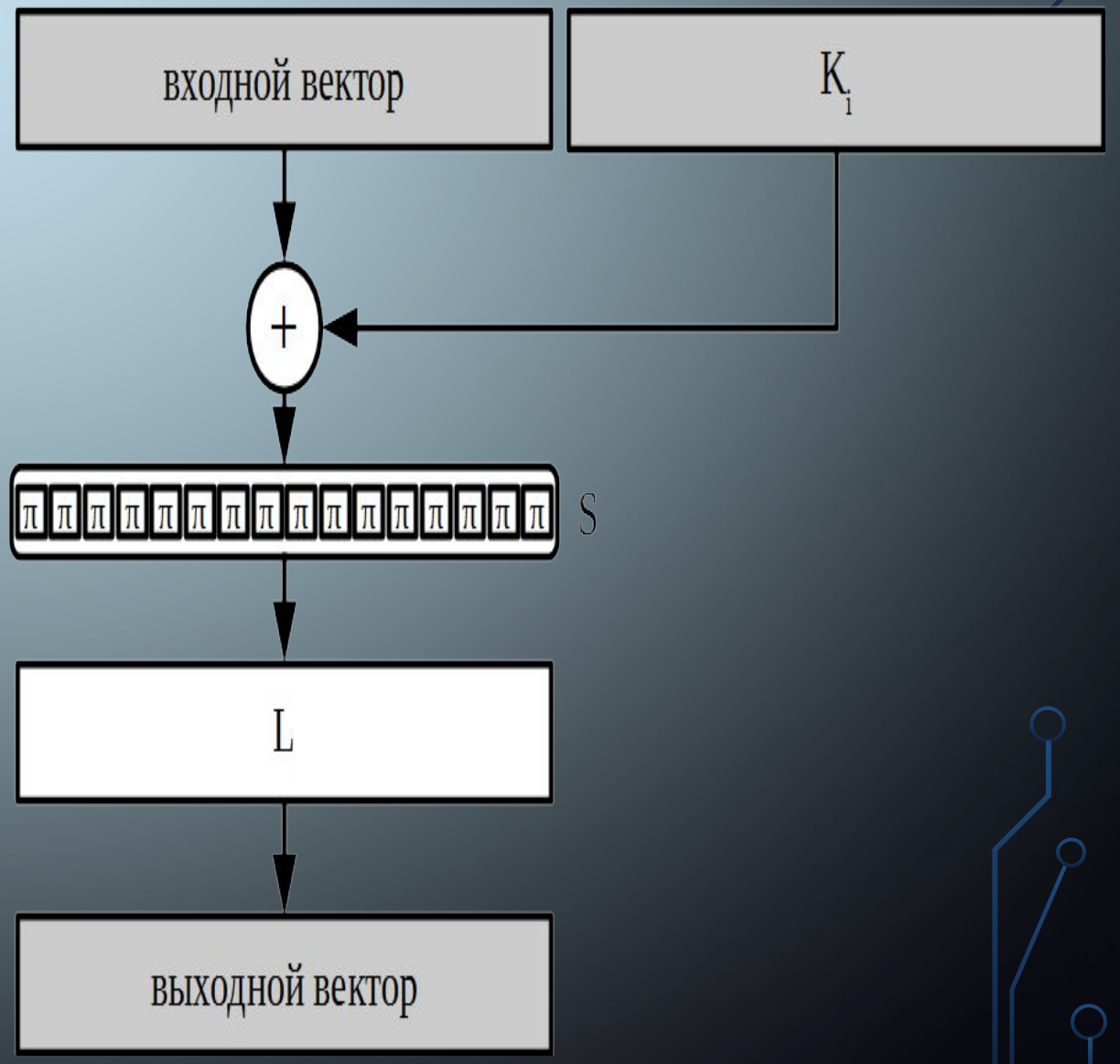
$F[k]: V_{128} \times V_{128} \rightarrow V_{128} \times V_{128}$

$F[k](a_1, a_0) = (LSX[k](a_1) \oplus a_0, a_1),$

где $k, a_0, a_1 \in V_{128}$.

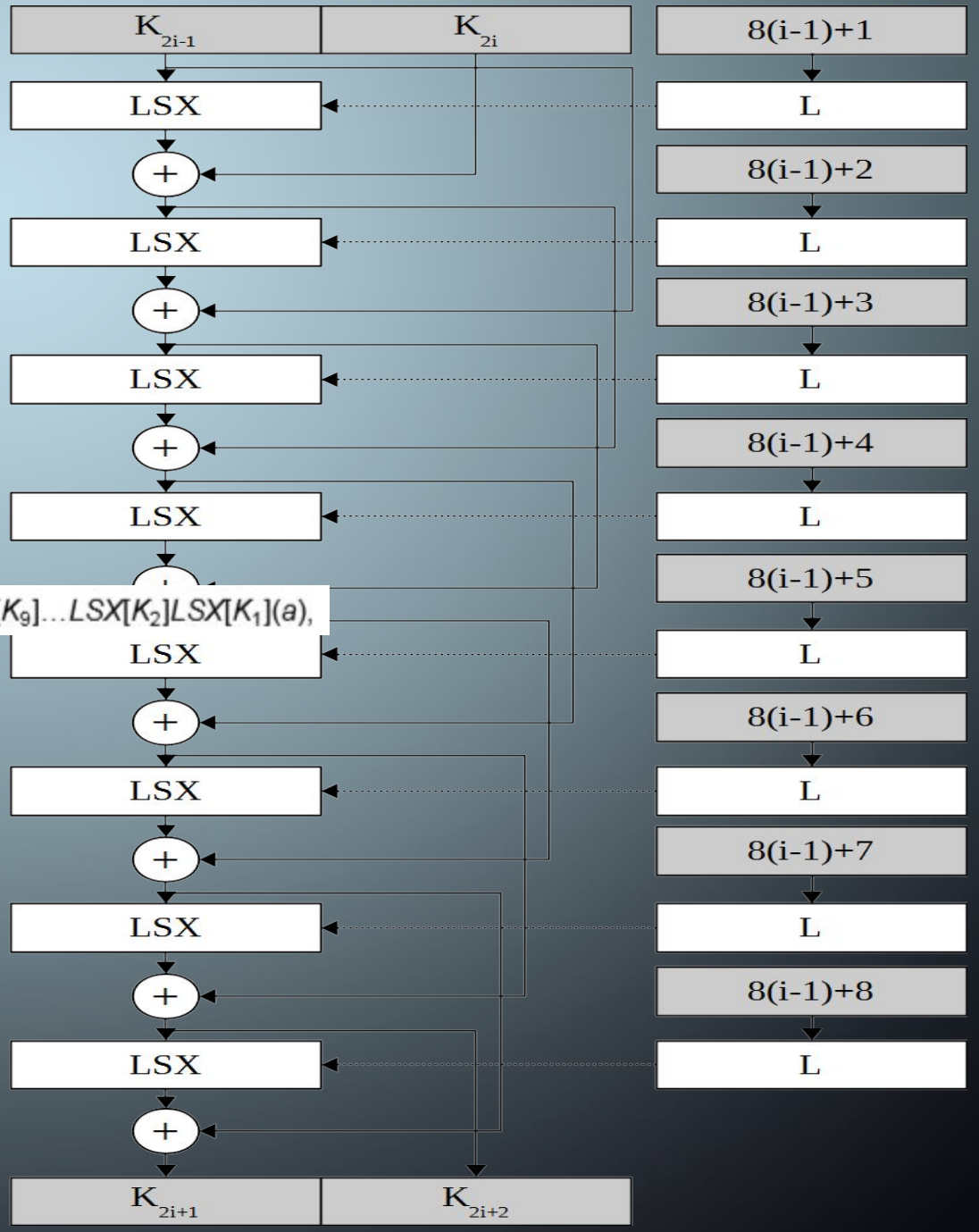
$$C_i = L(Vec_{128}(i)),\ i = 1, 2, \ldots, 32.$$

$$(K_{2i+1}, K_{2i+2}) = F[C_{8(i-1)+8}] \ldots F[C_{8(i-1)+1}](K_{2i-1}, K_{2i}),\ i = 1, 2, 3, 4.$$



РАУНД КЛЮЧЕВОЙ РАЗВЕРТКИ

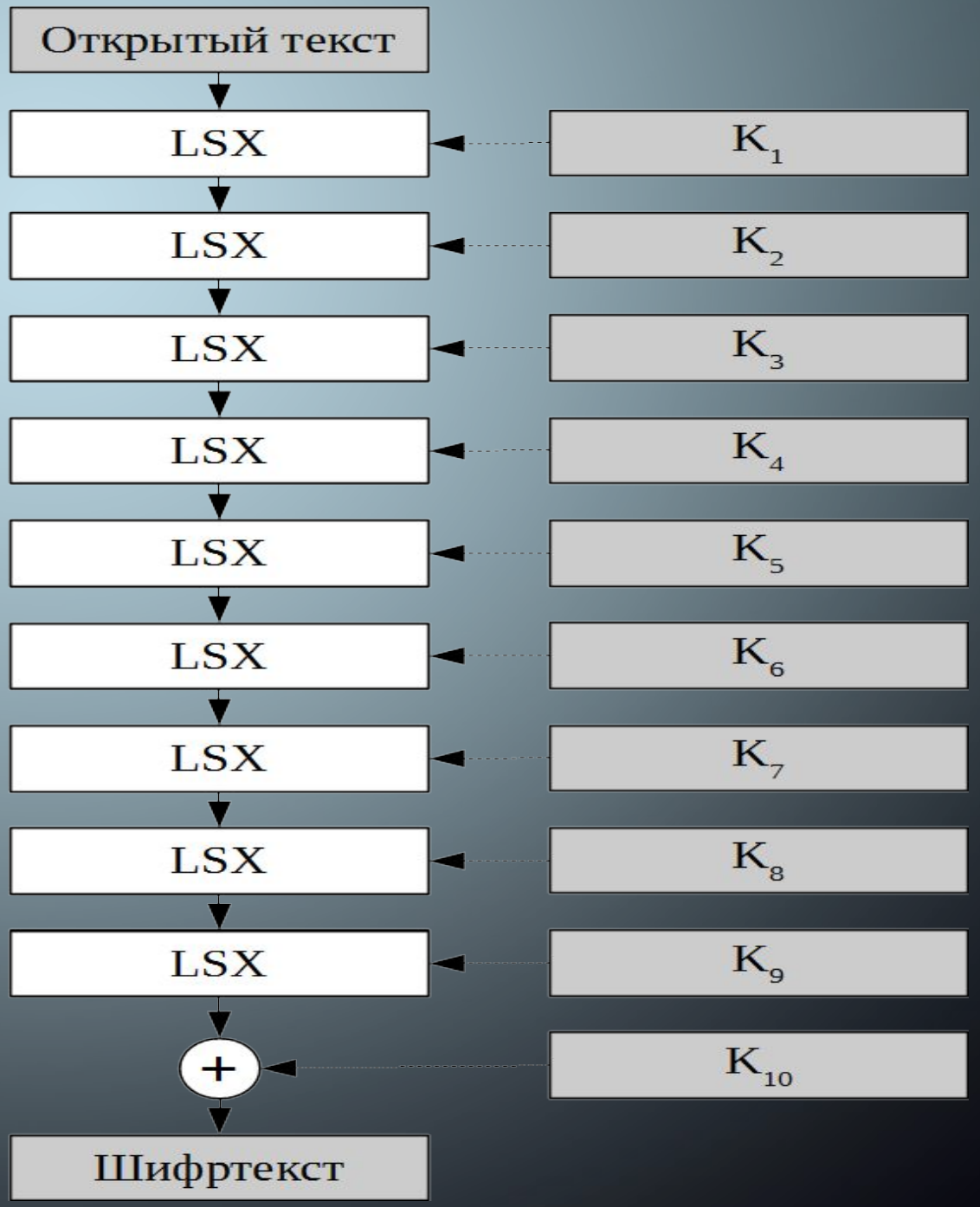
$$E_{K_1,\ldots,K_{10}}(a) = X[K_{10}]LSX[K_9]\ldots LSX[K_2]LSX[K_1](a),$$



В ВИДЕ БЛОК-СХЕМЫ:

Расшифрование реализуется обращением базовых преобразований и применением их в обратном порядке:

$$D_{K_1,\dots,K_{10}}(a) = X[K_1]S^{-1}L^{-1}X[K_2]\dots S^{-1}L^{-1}X[K_9]S^{-1}L^{-1}X[K_{10}](a),$$



«МАГМА» - АЛГОРИТМ БЛОЧНОГО ШИФРОВАНИЯ С ДЛИНОЙ БЛОКА N = 64 БИТ

- Длина шифруемого блока в алгоритме «Магма» — 64 бита. Длина ключа шифрования — 256 бит.
- На рисунке показана схема работы алгоритма при зашифровывании

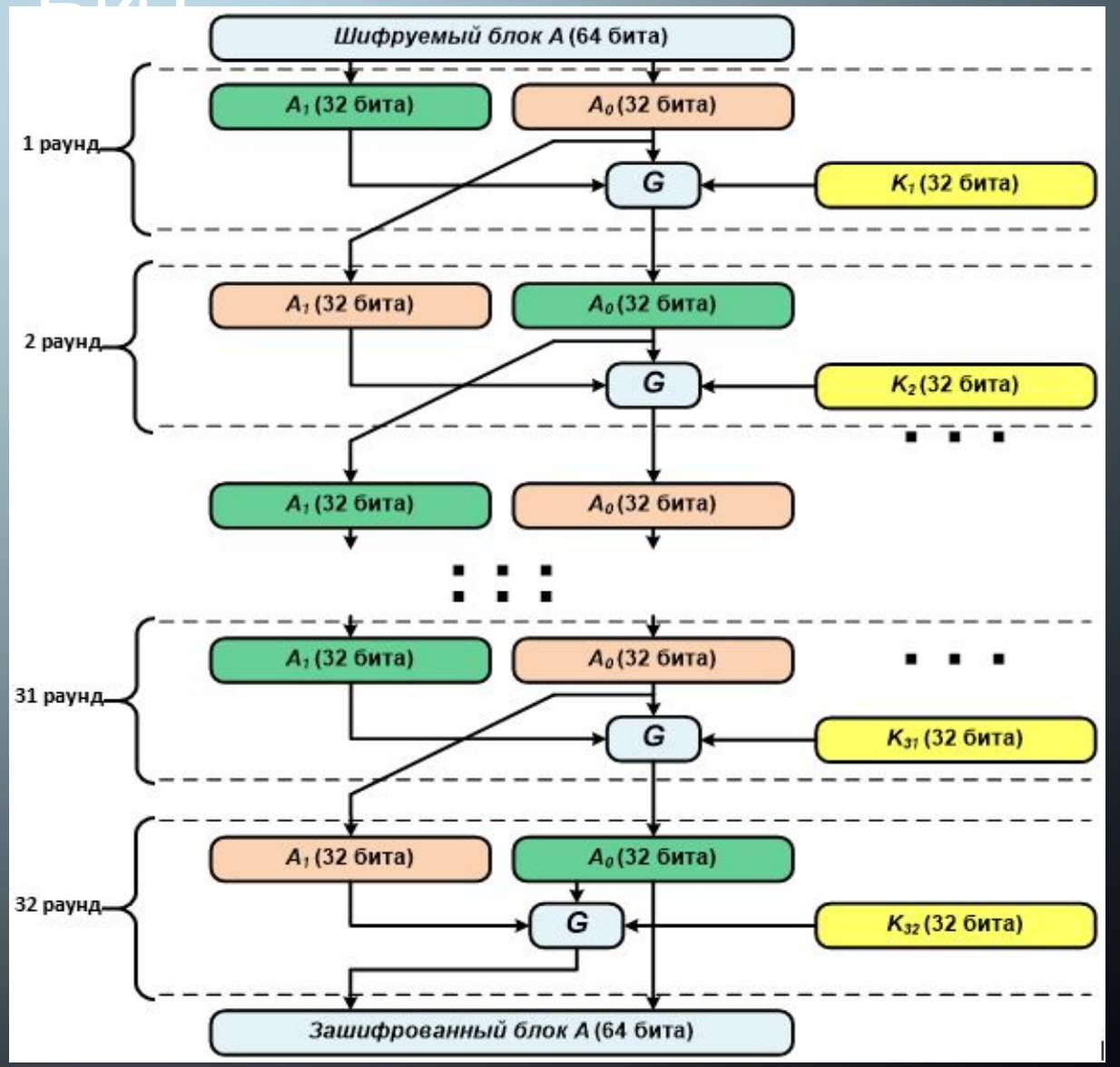


СХЕМА ОДНОЙ ИТЕРАЦИИ

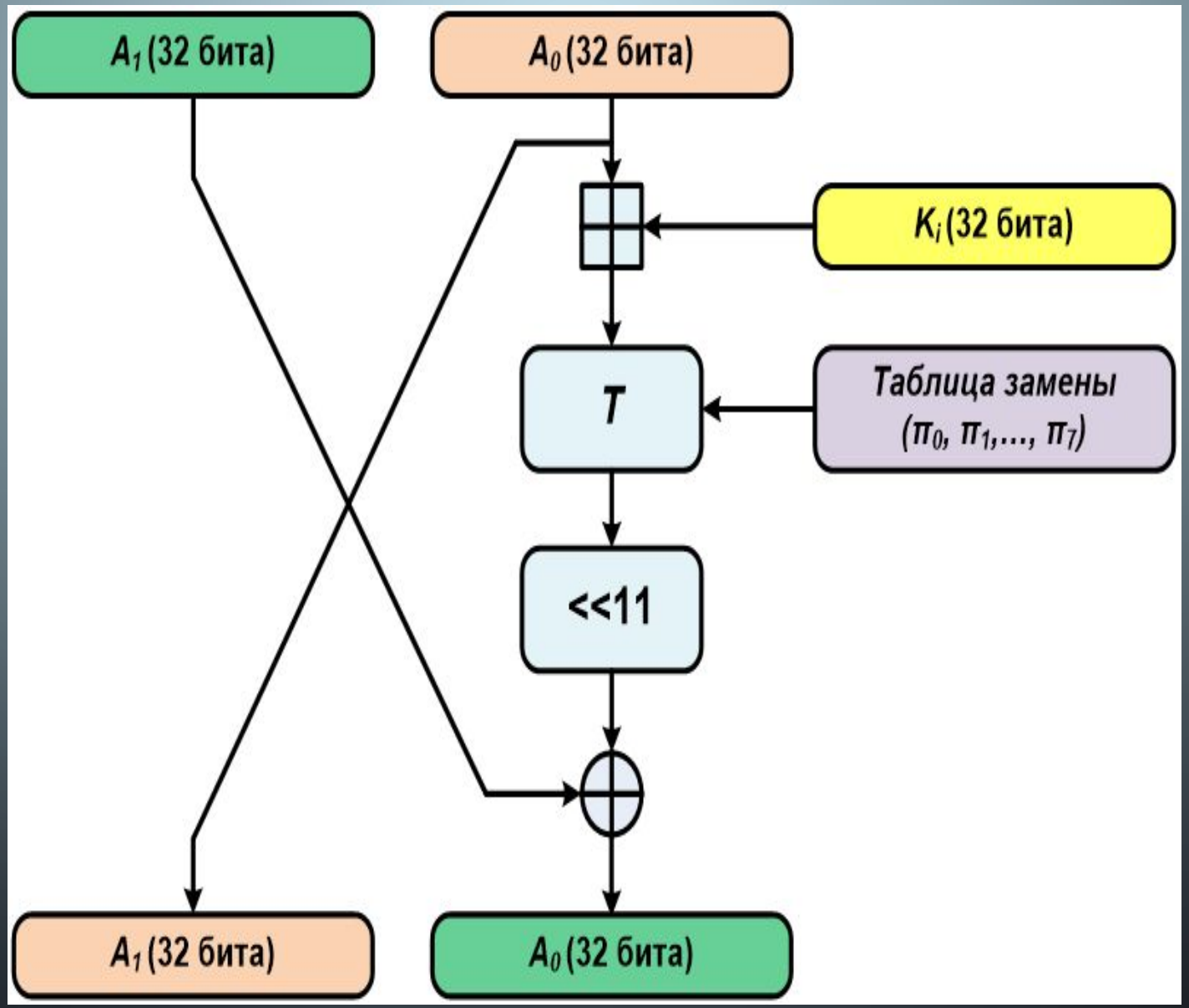


СХЕМА ПОЛУЧЕНИЯ ИТЕРАЦИОННЫХ КЛЮЧЕЙ

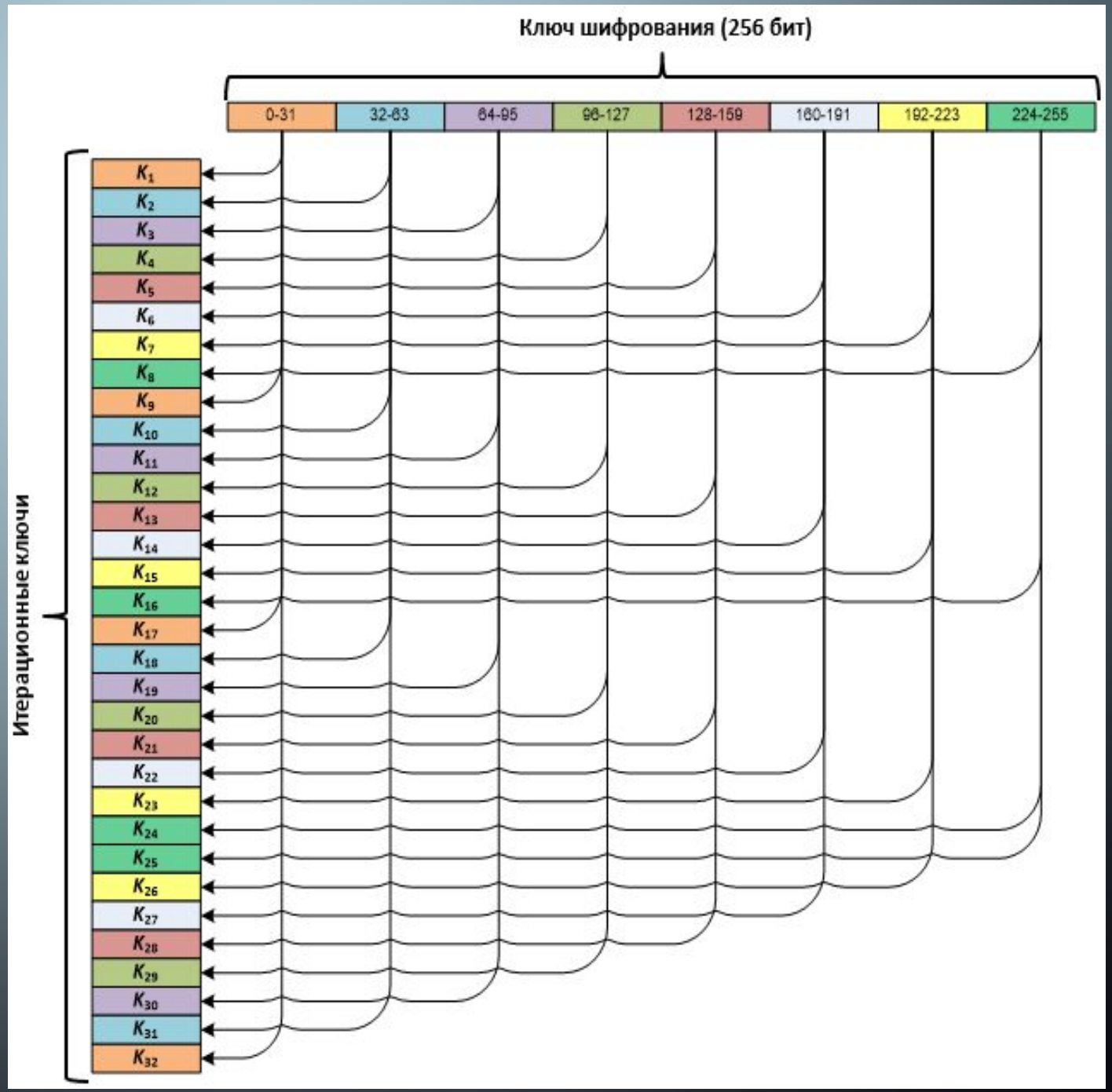
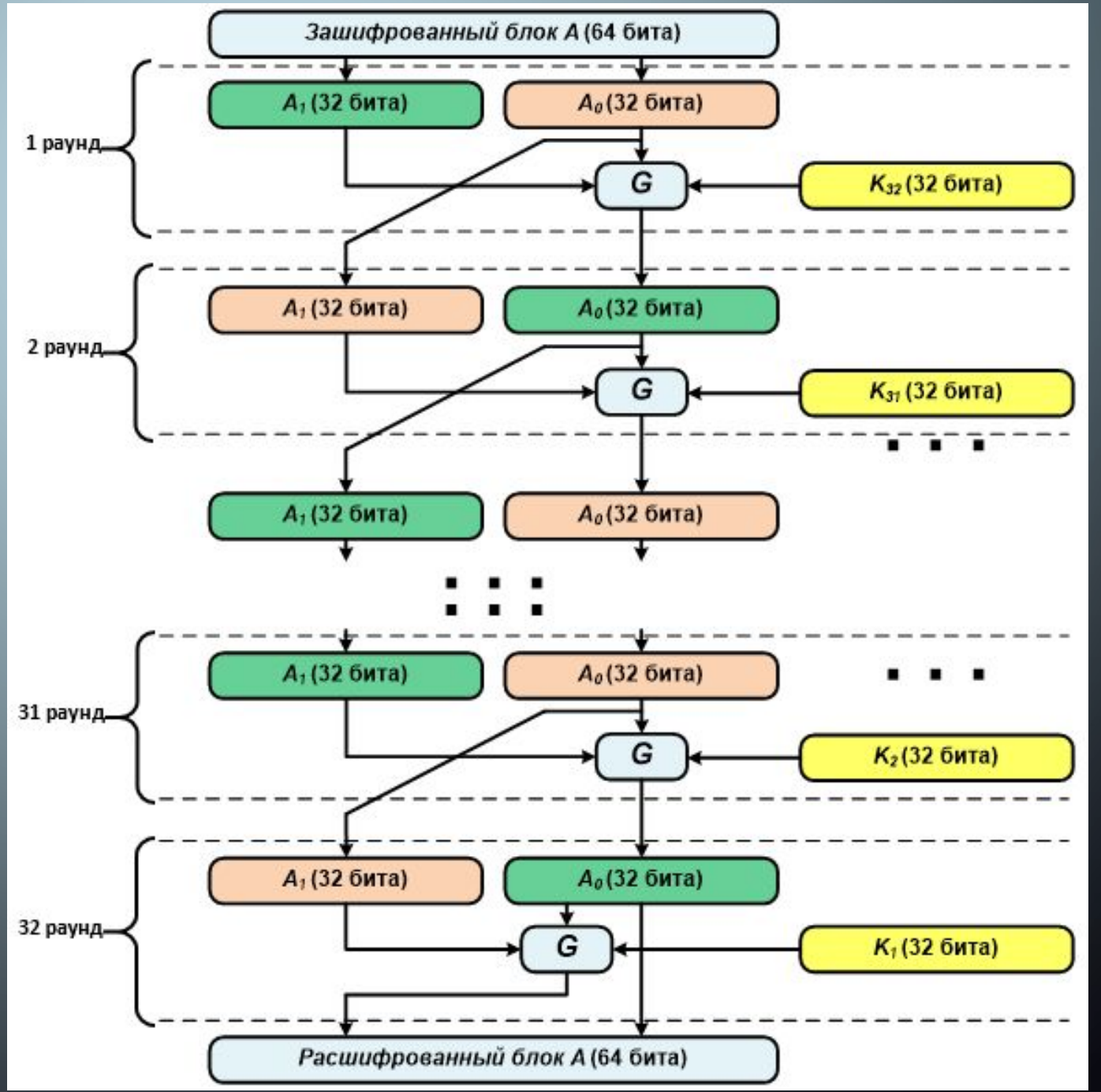


СХЕМА РАБОТЫ АЛГОРИТМА ПРИ РАСШИФРОВЫВАНИИ



СРАВНЕНИЕ ГОСТ 28147-89 И ГОСТ 34.12-2015

Алгоритм «Кузнечик» более современный и теоретически более стойкий, чем алгоритм «Магма» (который, по сути, практически без изменений был взят из старого ГОСТ 28147—89)

СПИСОК ЛИТЕРАТУРЫ

- ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».
- ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры»
- Мельников В. В. Защита информации в компьютерных системах. — М.: Финансы и статистика, 1997.
- Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. — М.: Радио и связь, 1999.
- Харин Ю. С., Берник В. И., Матвеев Г. В. Математические основы криптологии. — Мн.: БГУ, 1999.

СПАСИБО ЗА ВНИМАНИЕ!