Лекция
Стандарт шифрования ГОСТ 28147-89

- Лектор: профессор Яковлев В.А.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ
СОЮЗА ССР

СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ. ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ

АЛГОРИТМ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

ГОСТ 28147—89

Издание официальное

ИПК ИЗДАТЕЛЬСТВО СТАНДАРТОВ
Москва

Назначение

Алгоритм криптографического преобразования данных предназначен для обеспечения конфиденциальности и целостности информации в компьютерных сетях, отдельных вычислительных комплексах и ЭВМ

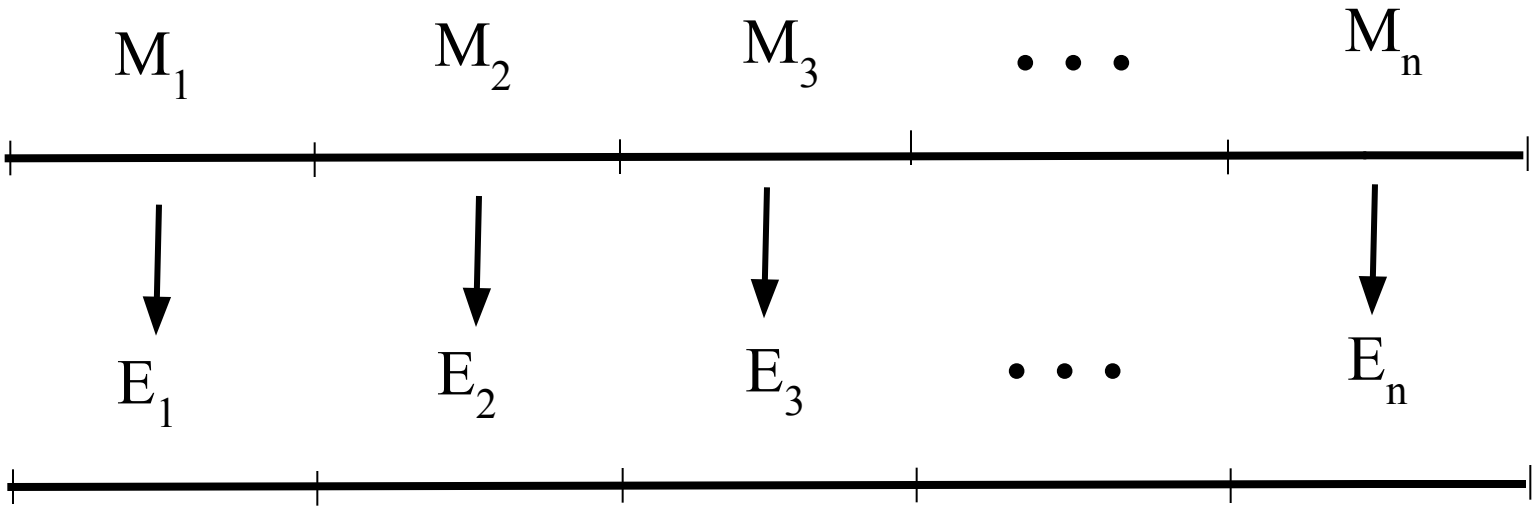
Назначение

Алгоритм криптографического преобразования данных предназначен для обеспечения конфиденциальности и целостности информации в компьютерных сетях, отдельных вычислительных комплексах и ЭВМ

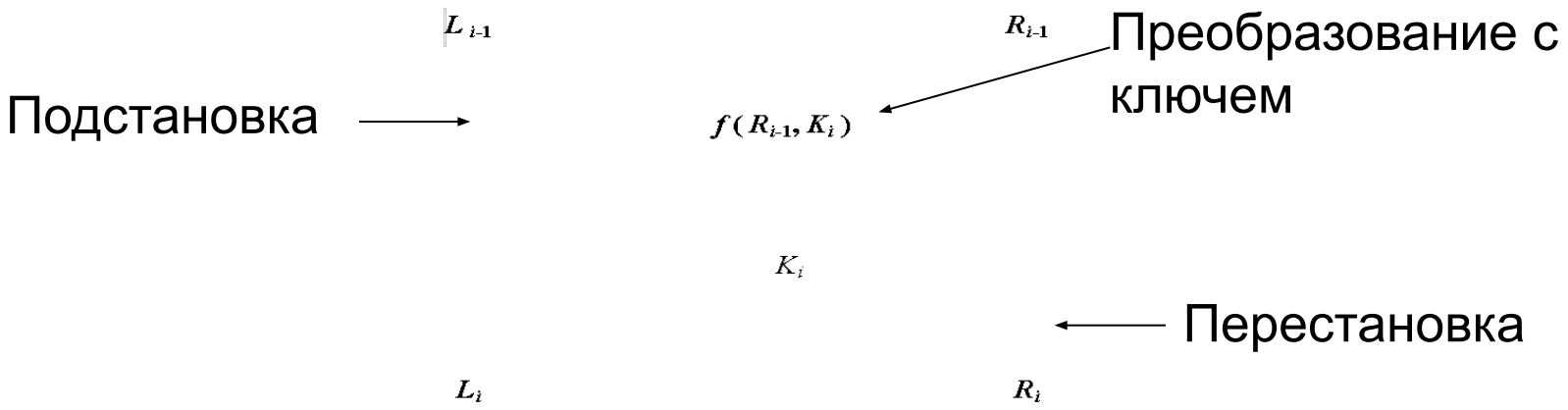
Блочные шифры

Наименование шифра	Год	Длина ключа	Схема
DES	1975	56	F
FEAL	1978	64	F
ГОСТ 28147-89	1989	256	F
IDEA	1991	128	
BLOWFISH	1993	32-448	F
RC5 (RC6)	1994	255	
AES	2000	128-256	

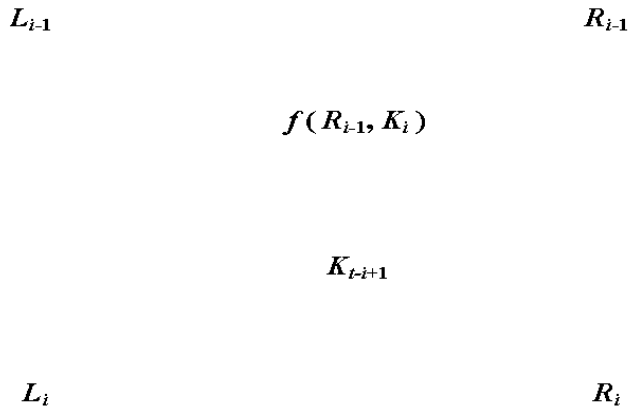
Принцип блочного шифрования



Алгоритм шифрования - схема Файстеля



Одна итерация шифрования



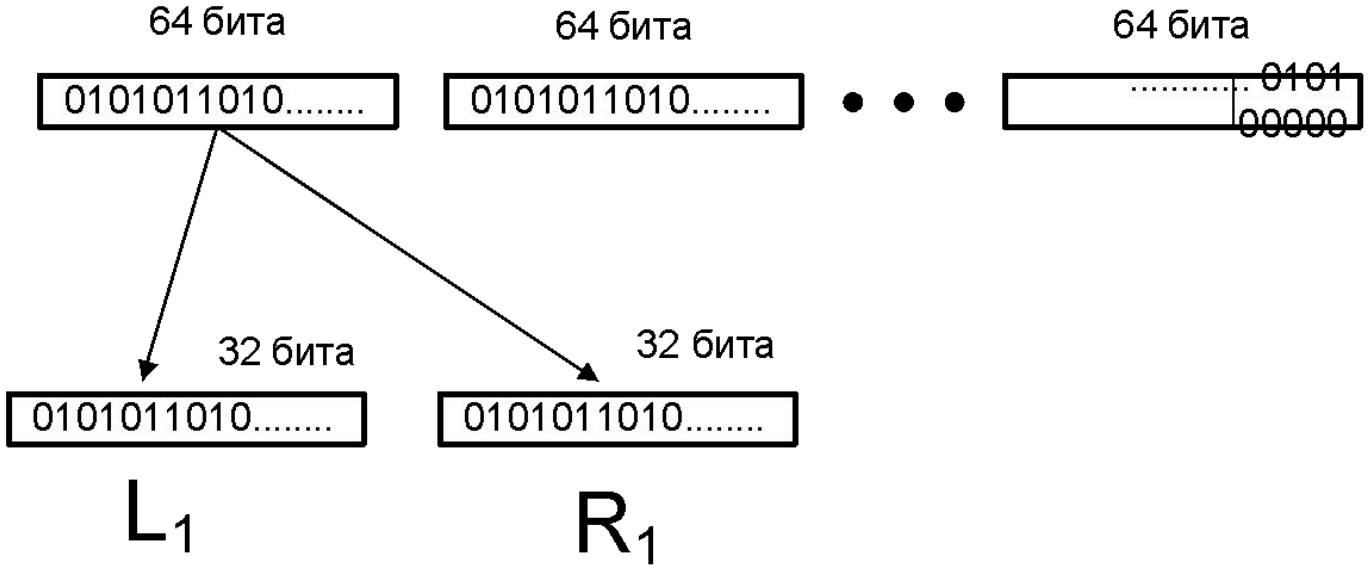
Одна итерация расшифрования

Режимы работы алгоритма

1. шифрование данных в режиме простой замены;
2. шифрование данных в режиме гаммирования;
3. шифрование данных в режиме гаммирования с обратной связью;
4. выработка имитовставки.

Исходное сообщение

Сообщение разбивается на блоки по 64 бита



Основные параметры алгоритма шифрования

- Длина шифруемого блока - 64 бита
- Длина ключа - 256 бит
- Число раундов шифрования -32
- Длина блока(машинного слова) для выполнения преобразований -32 разряда
- Реализация - программная, программно-аппаратная.

Режимы работы алгоритма

1. шифрование данных в режиме простой замены;
2. шифрование данных в режиме гаммирования;
3. шифрование данных в режиме гаммирования с обратной связью;
4. выработка имитовставки.

Шифрование в режиме простой замены

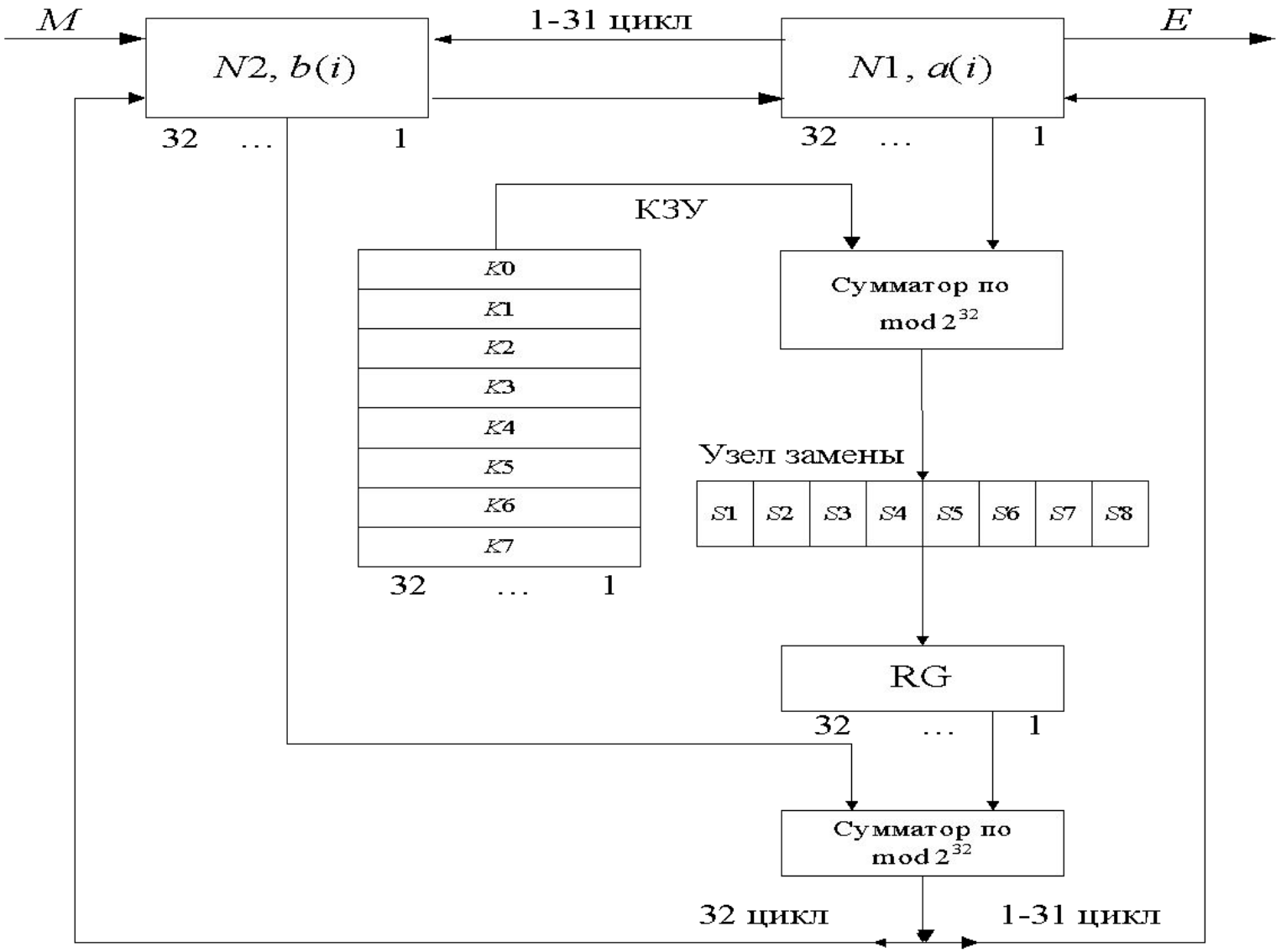


Таблица замены

Вход S_1	Выход S_1
0000	1011
0001	1111
0010	1110
0011	0100
0100	1101
0101	1001
0110	0010
0111	1010
1000	0011
1001	0111
1010	0001
1011	1100
1100	0000
1101	0110
1110	0101
1111	1000

Уравнения преобразований

$a(j) = \{f\,[(a(j-1) + K_{(j-1)} \bmod 8) \bmod 2^{32}] + b(j-1)\} \bmod 2,$
$b(j) = a(j-1);$ при $j = 1, \ldots, 24;$

$a(j) = \{f\,[a(j-1) + K_{32-j}] \bmod 2^{32} + b(j-1)\} \bmod 2,$
$b(j) = a(j-1),$ при $j = 25, \ldots, 31;$

$a(32) = a(31),$
$b(32) = \{f\,[a(31) + K_0]) \bmod 2^{32} + b(31)\} \bmod 2,$ при $j = 32.$

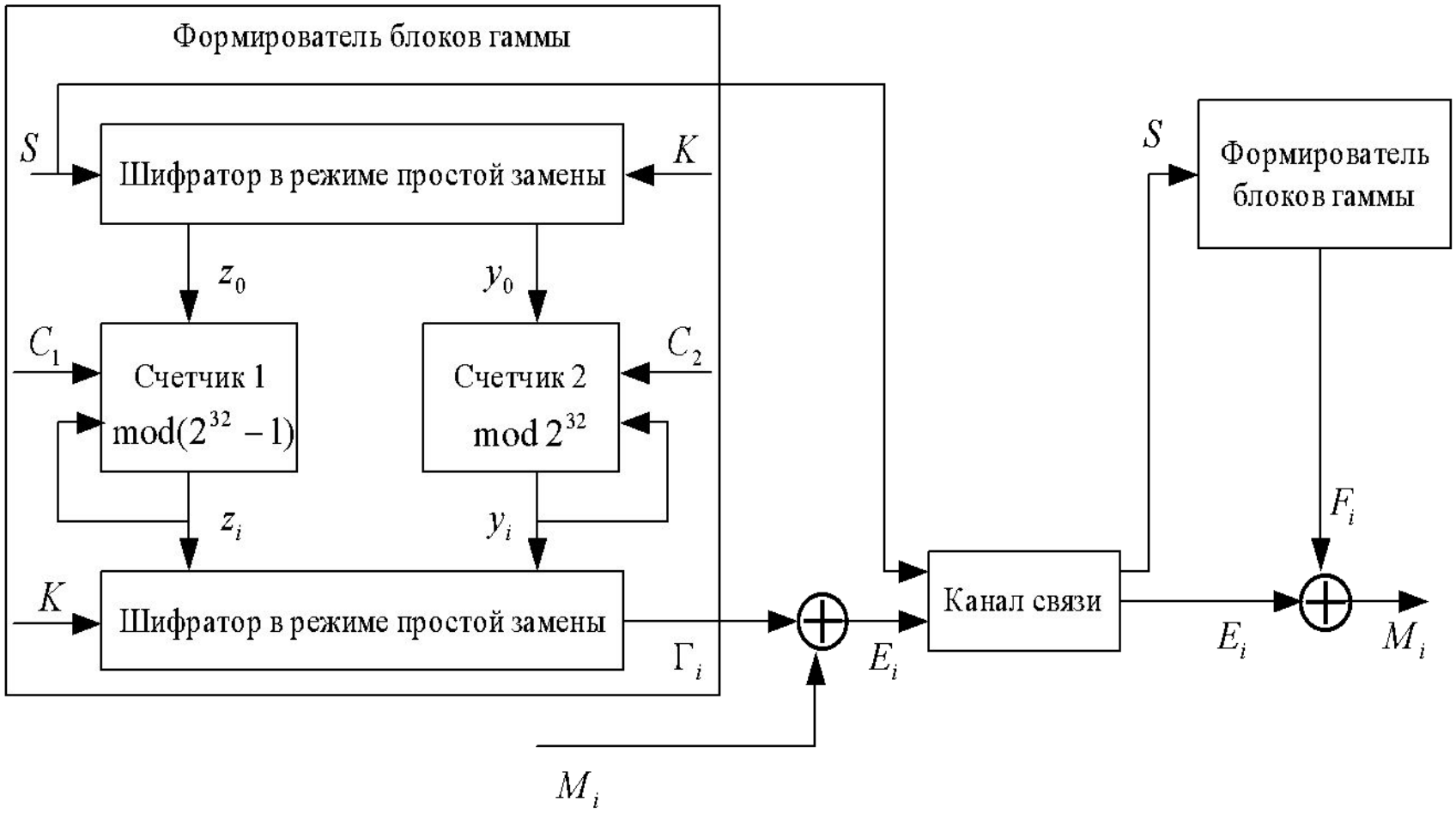
Достоинства и недостатки режима

Достоинства алгоритма: простота реализации как аппаратным, так и программным способом.

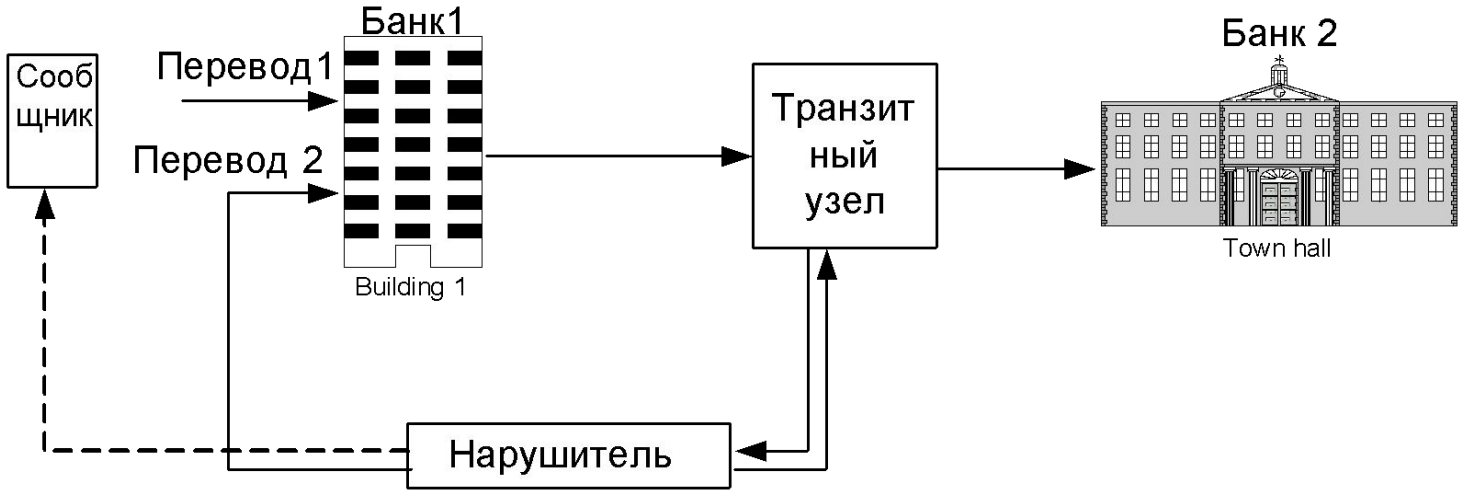
Недостатки:

1. Шифрование одинаковых блоков исходного текста дает идентичные блоки шифрованного текста, что позволяет сделать выводы о свойствах исходного текста.
2. При расшифровании криптограммы происходит размножение ошибок, возникших в ней при передаче по каналу связи.
3. Возможна модификация сообщения путем перестановки блоков криптограммы.

Шифрование в режиме гаммирования



Вариант подмены зашифрованных сообщений в режиме кодовой книги



Номер блока

1	2	3	4	5	6	7	8	9	10	11	12	13
Метка времени	Бланк-по-лучатель	Банк-от-правитель		Имя вкладчика						Счет вкладчика		Сумма

Поле

Достоинства и недостатки режима

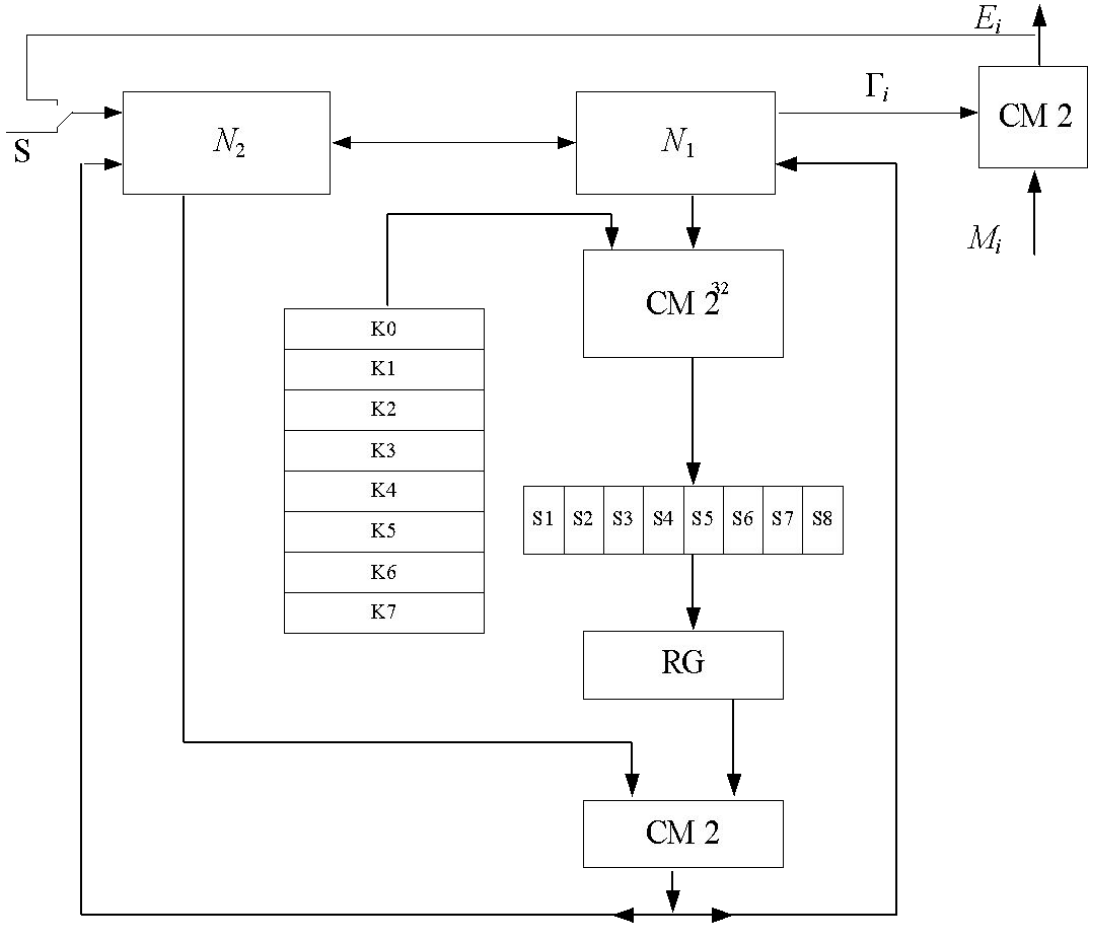
Достоинства алгоритма: 1. реализация также проста, как и для режима простой замены.

2. Решена проблема повторений, возникающих при зашифровании одинаковых блоков сообщения.
3. Перестановки блоков текста также будут обнаружены.
4. При расшифровании криптограммы не происходит размножение ошибок, возникших в ней при передаче по каналу связи.

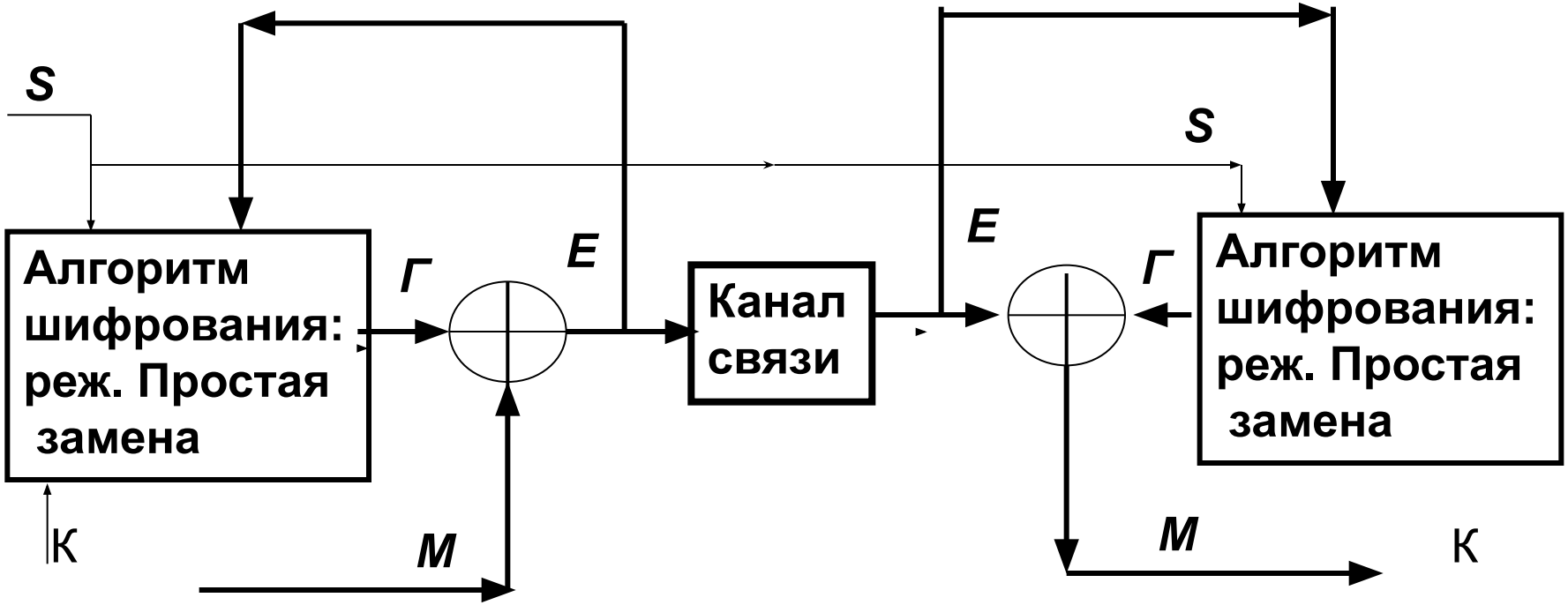
Недостатки:

1. Возможна модификация сообщения путем наложения на криптограмму ложного сообщения. $E'=E+M_л$
2. Требуется формирование и передача на приемную сторону синхропосылки.

Шифрование в режиме гаммирования с обратной связью



Шифрование в режиме гаммирования с обратной связью



Достоинства и недостатки режима

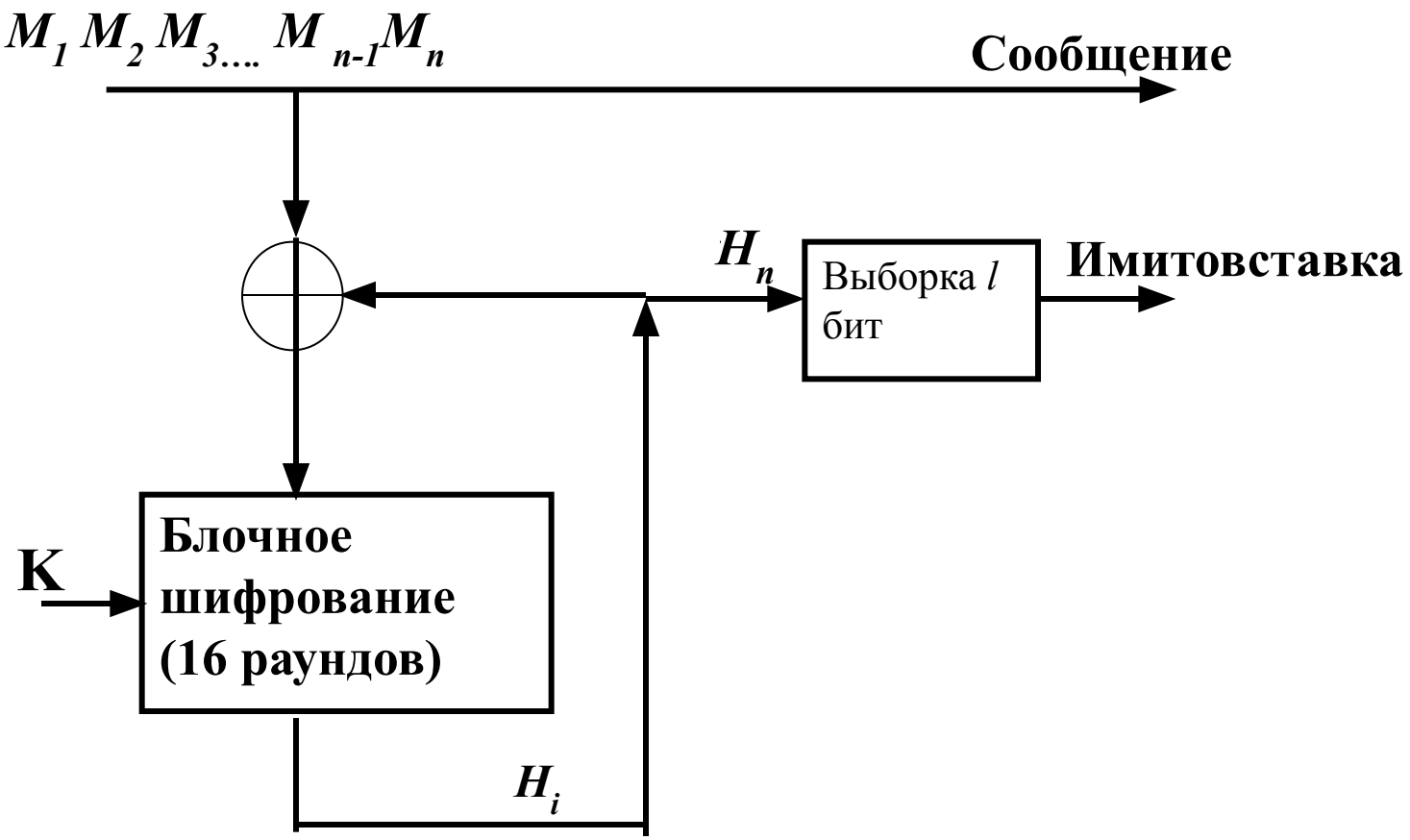
Достоинства алгоритма:

1. Обеспечивается устойчивость к перестановке блоков криптограммы и навязыванию путем наложения, так как блоки криптограммы оказываются связанными между собой.
2. Обеспечивается самосинхронизация шифратора и дешифратора после приема первого блока криптограммы.

Недостатки:

1. Требуется формирование и передача на приемную сторону синхропосылки.
2. При расшифровании криптограммы происходит удвоенное размножение ошибок, возникших в ней при передаче по каналу связи.

Выработка имитовставки



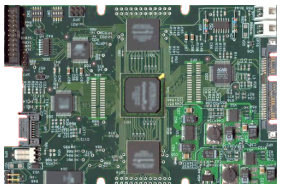
Устройства криптографической защиты «Криптон»

Производитель ООО Фирма «Анкад»

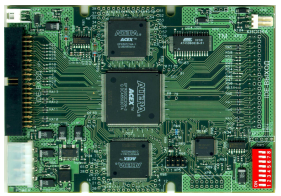
г. Зеленоград Московская Обл.

КРИПТОН-8

КРИПТОН-4/PCI

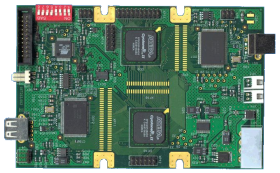


КРИПТОН SATA

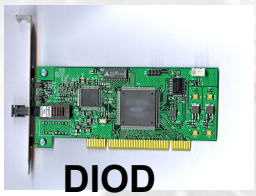


КРИПТОН IDE

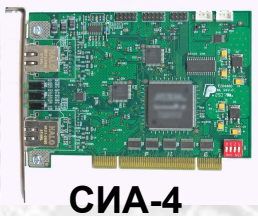
КРИПТОН USB



КРИПТОН USB HS

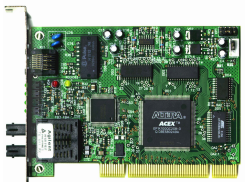


DIOD



СИА-4

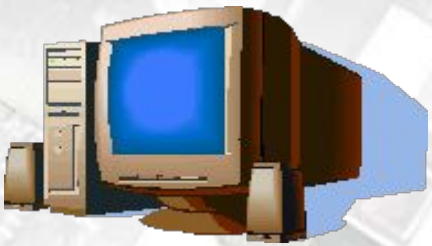
КРИПТОН AncNet



AncNet

Сетевые устройства

Универсальные (абонентские) шифраторы

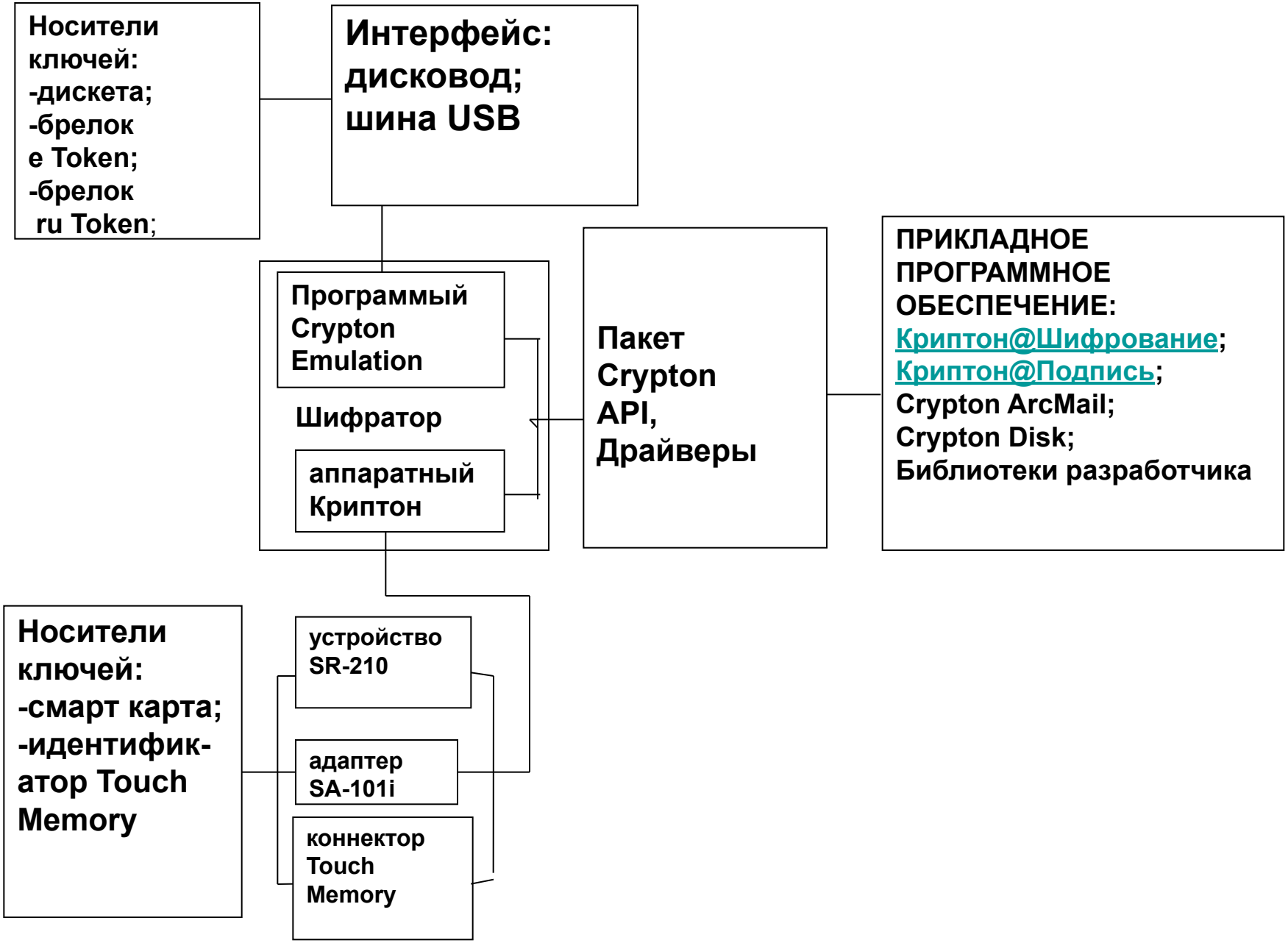


Средства ограничения и разграничения доступа

КРИПТОН-ЗАМОК

Дисковые шифраторы

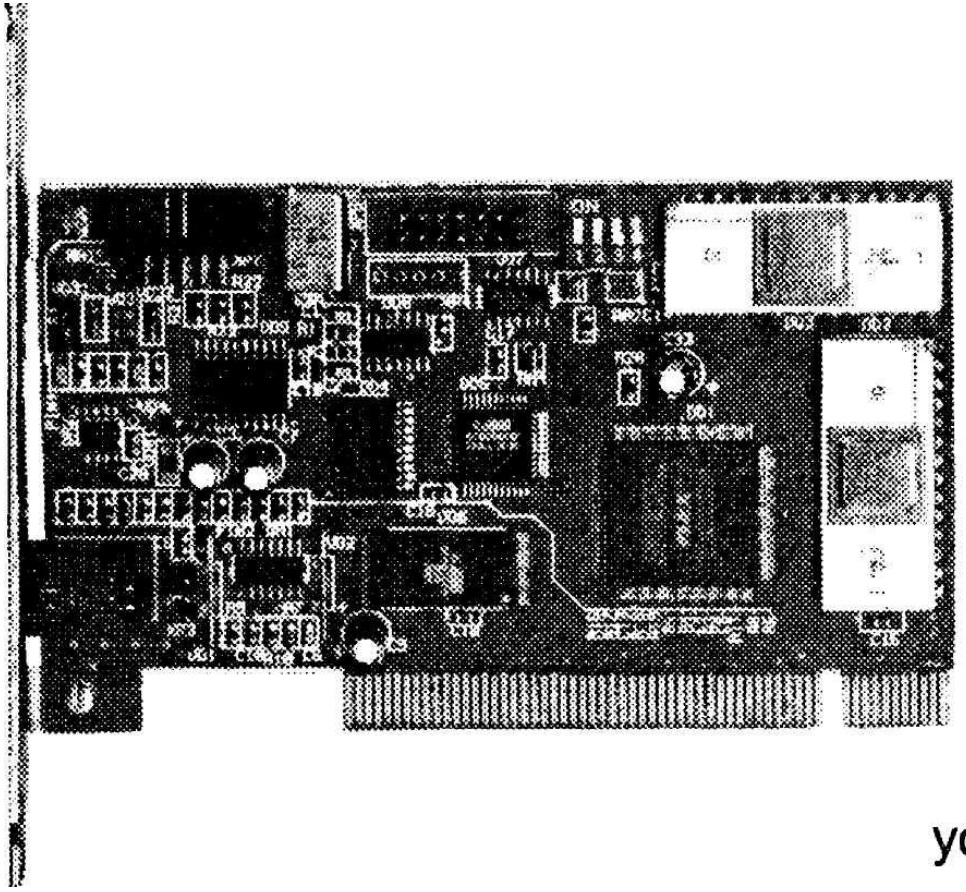
Система криптографической защиты информации КРИПТОН



Технические характеристики УКЗД КРИПТОН

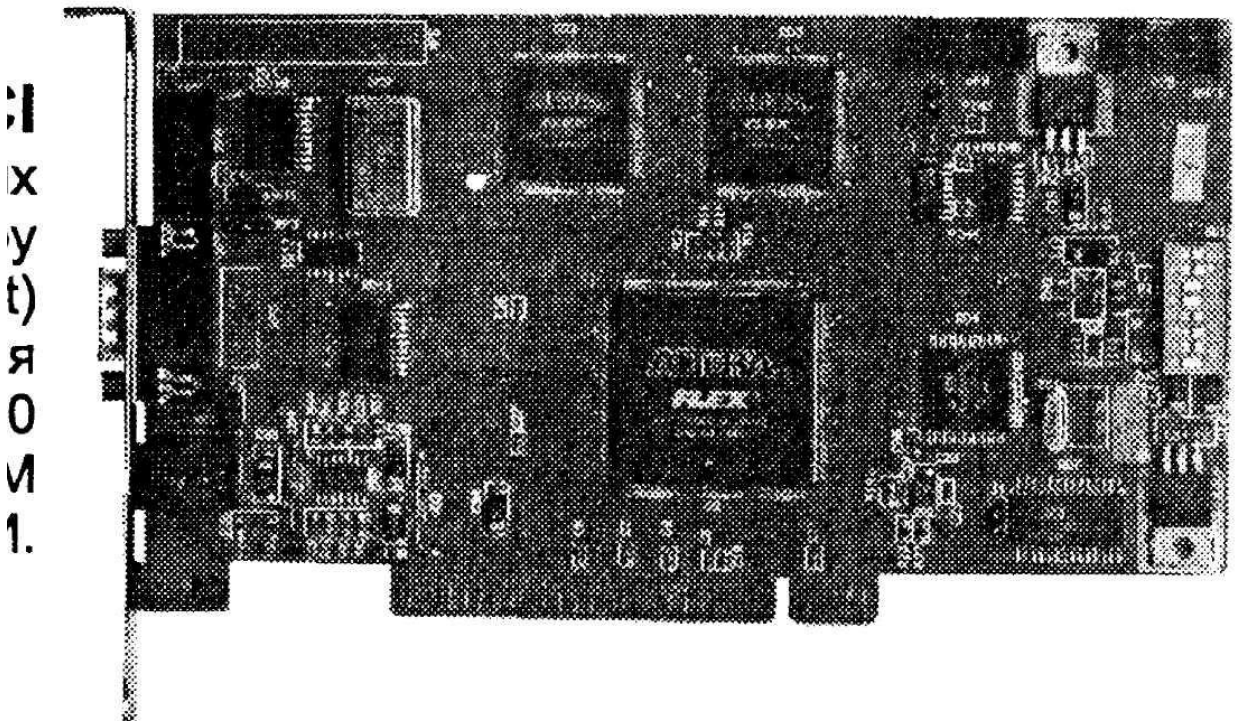
Технические характеристики	**Криптон –4/PCI**	**Криптон –8/PCI**	**Криптон –9/PCI**
Шина	**PCI(Target)**	**PCI(Target, Bus Master)**	**PCI(Bus Master)**
Скорость шифрования (кБайт/с)	**до 1100**	**до 8500**	**до 10000**
Носители ключей	**Дискеты, СК,ТМ**	**Дискеты, СК,ТМ**	**Дискеты,СК, ТМ**
Стоимость $	420	470	520

Криптон 4/PCI

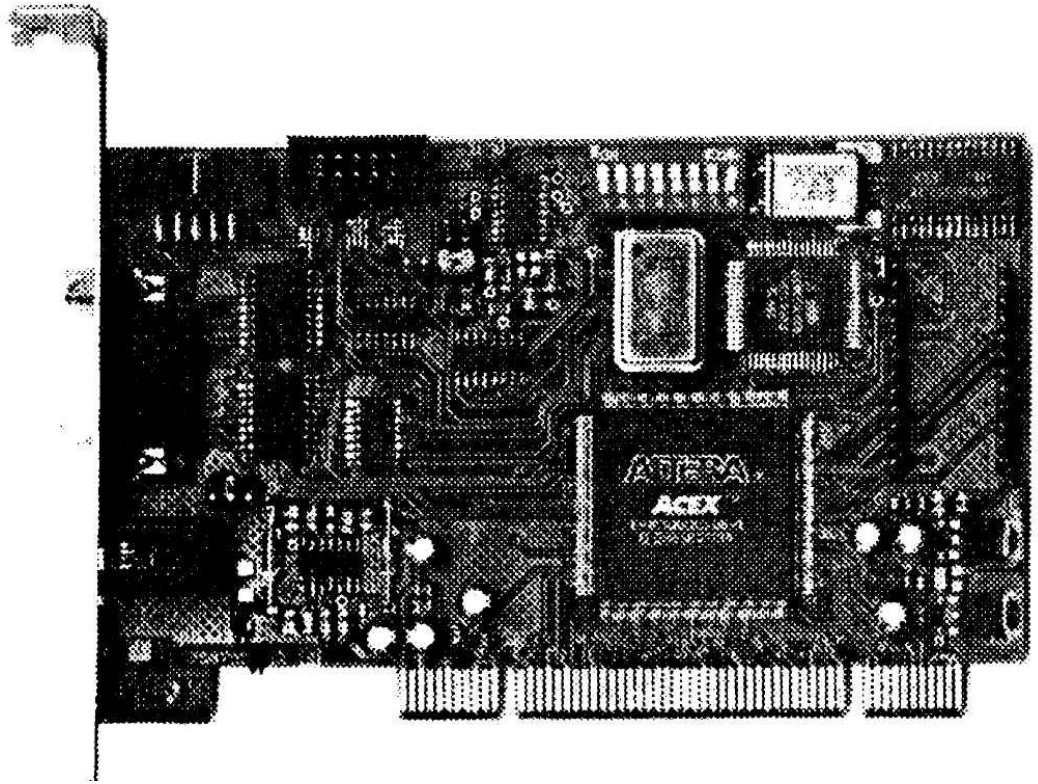


уст

Криптон 8/PCI



Криптон 9/PCI



Архитектура ключей системы КРИПТОН

Архивное шифрование

Архивное шифрование
применяется для шифрования данными, обмен которыми не предполагается

Основная система (0): файл □ ФК □ ПК □ ГК□ П

ФК - файловый ключ,
ПК(UK) - пользовательский ключ,
ГК(GK) - главный ключ,
П(PW) - пароль.

Разновидности архивной системы:
(1) файл □ ФК □ ПК □ ГК
(4) файл □ ФК □ ПК □П
(5) файл □ ФК □ ПК

Сетевое шифрование

Сетевое шифрование предназначено для шифрования файлов, передаваемых в сети связи

а). Распределение ключей

Главный узел сети связи создает Сетевую таблицу (СТ), которая шифруется Ключем сетевой таблицы (КСТ)

номера узлов	1	2	i	M
1	$К_{11}$	$К_{12}$	$К_{1i}$	$К_{1M}$
2	$К_{21}$	К22	$К_{2i}$	$К_{2M}$
j	$К_{j1}$	$К_{j2}$	Кji	$К_{jM}$
M	$К_{M1}$	$К_{M2}$	$К_{Mi}$	$К_{MM}$

$К_{ij}$= $К_{ji}$ – сетевой ключ (СК) для связи i-го узла с j-м и наоборот

Каждая строка таблицы представляет Сетевой набор (СН), т.е набор ключей, обеспечивающий криптографическую связность данного узла с другими узлами сети.

При копировании Сетевого набора на носитель –дискету, набор шифруется на ключе сетевого набора (КСН).

Дискеты с Сетевыми наборами распределяются между узлами сети с помощью курьеров.

б). Передача файлов

файл □ ФК □ СК □ КСН □ ГК □ П

Шифрование в режиме простой замены

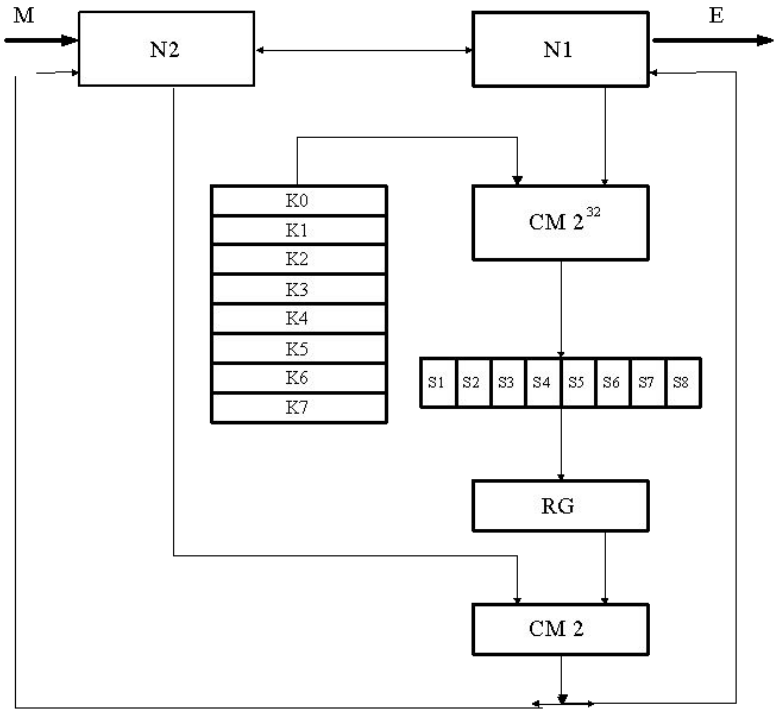


Рис. 1. Структурная схема алгоритма шифрования в режиме простой замены