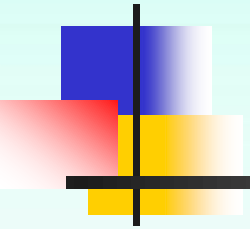
CRYPTOGRAPHY



МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Лек. 13 2022 КІБ-19

СТАНДАРТ ДСТУ 7624:2014 «КАЛІНА»

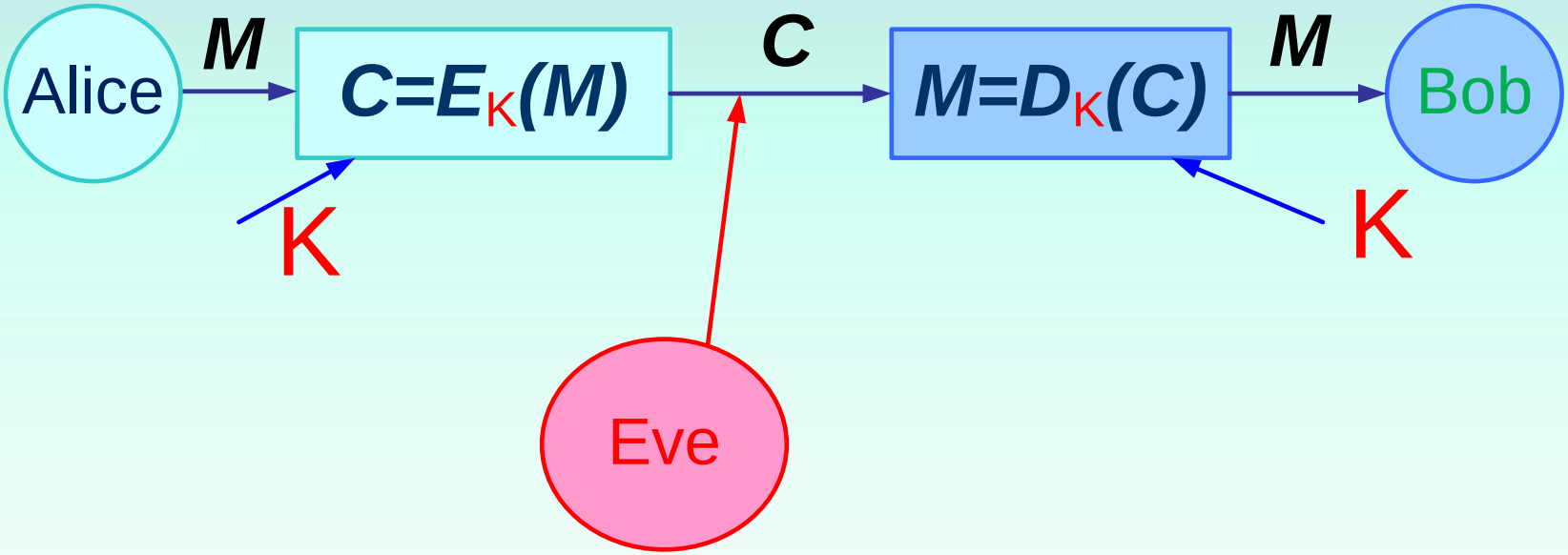
«КАЛИНА»

1. Достоинства и недостатки AES.
2. Развитие симметричных стандартов
3. Стандарт «Калина»

Режимы блочного шифрования

1. ECB – Electronic Codebook.
2. CBC – Cipher Block Chaining
3. PCBC – Propagating CBCCFB
4. CFB - Cipher Feedback
5. OFB – Output Feedback
6. CTR – Counter Mode
7. GCM – Galois|Counter Mode

Симметричное шифрование



СИММЕТРИЧНЫЙ АЛГОРИТМ
→ ОДИН СЕКРЕТНЫЙ КЛЮЧ

как для шифрования, так и дешифрования

Преимущества AES

Рассеивание — изменение любого знака ключа или открытого текста влияет на большое количество знаков шифротекста.

Перемешивание — используемые преобразования затрудняют получение статистических зависимостей между открытым и закрытым текстом.

Не подвержен многим видам криптоаналитических атак, таких как: дифференциальный криптоанализ, линейный криптоанализ, square — атака.

Байт-ориентированная структура, что дает хорошие перспективы для реализации алгоритма в будущих процессорах.

Высокое **быстродействие** на различных платформах.

«Недостатки» AES

Известны **теоретические** атаки со сложностью, меньше, чем полный перебор;

Не может в полной мере использовать возможности **64-битных платформ**;

Отсутствие доверия **к иностранным аппаратных реализаций** AES (в том числе набора инструкций AES-NI процессоров x86 и x86_64) на основе данных Э. Сноудена.

*Мировые лидеры ИТ-индустрии начали постепенно отказываться от **AES**, например, компания Google в 2014 году внедрила на замену алгоритм ChaCha20 для защиты каналов связи мобильных устройств на базе операционной системы Android.*

Стандарты на базе AES

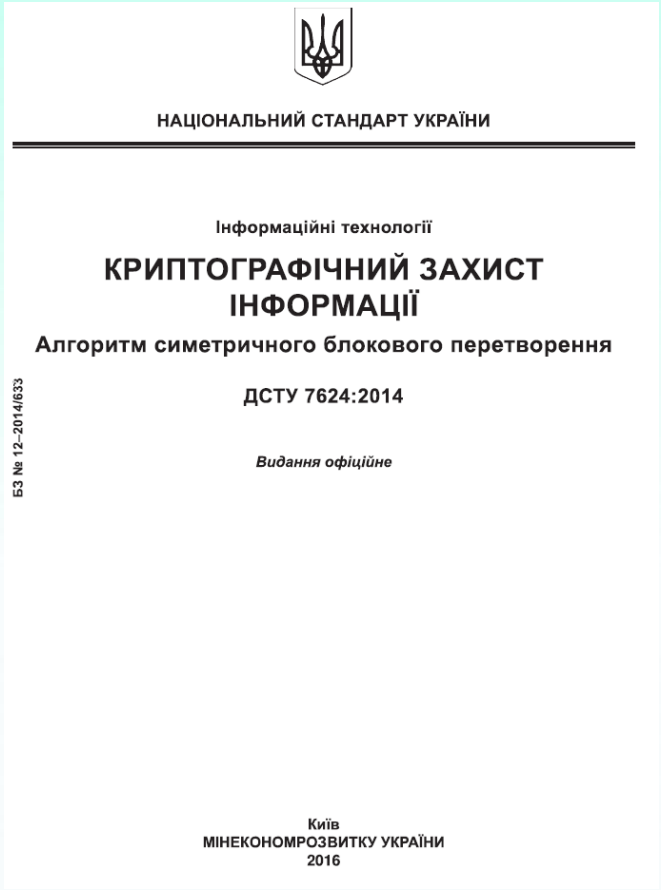
Белоруссия. СТБ 34.101.31-2011

- Блок 128 бит. Ключ 128, 192, 256 бит.
- 8 раундов (!! Фейстель)
- Один S блок
- Нет генерации раундовых ключей.

Российская Федерация. ГОСТ Р 34.12-2015 («Кузнечик»)

- Блок 128 бит. Ключ 256 бит.
- 9 раундов (подобно AES)
- Один S блок. Матрица линейного преобразования 16x16 над полем $\mathbf{2^8}$
- Генерации раундовых ключей на базе смесителя Фейстеля.
- Использование функций хеширования **(ГОСТ Р 34.11-2012 «Стрибог»)** для преобразований подстановки.

Стандарт ДСТУ 7624:2014 «Калина»



НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

Інформаційні технології

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Алгоритм симетричного блокового перетворення

ДСТУ 7624:2014

Видання офіційне

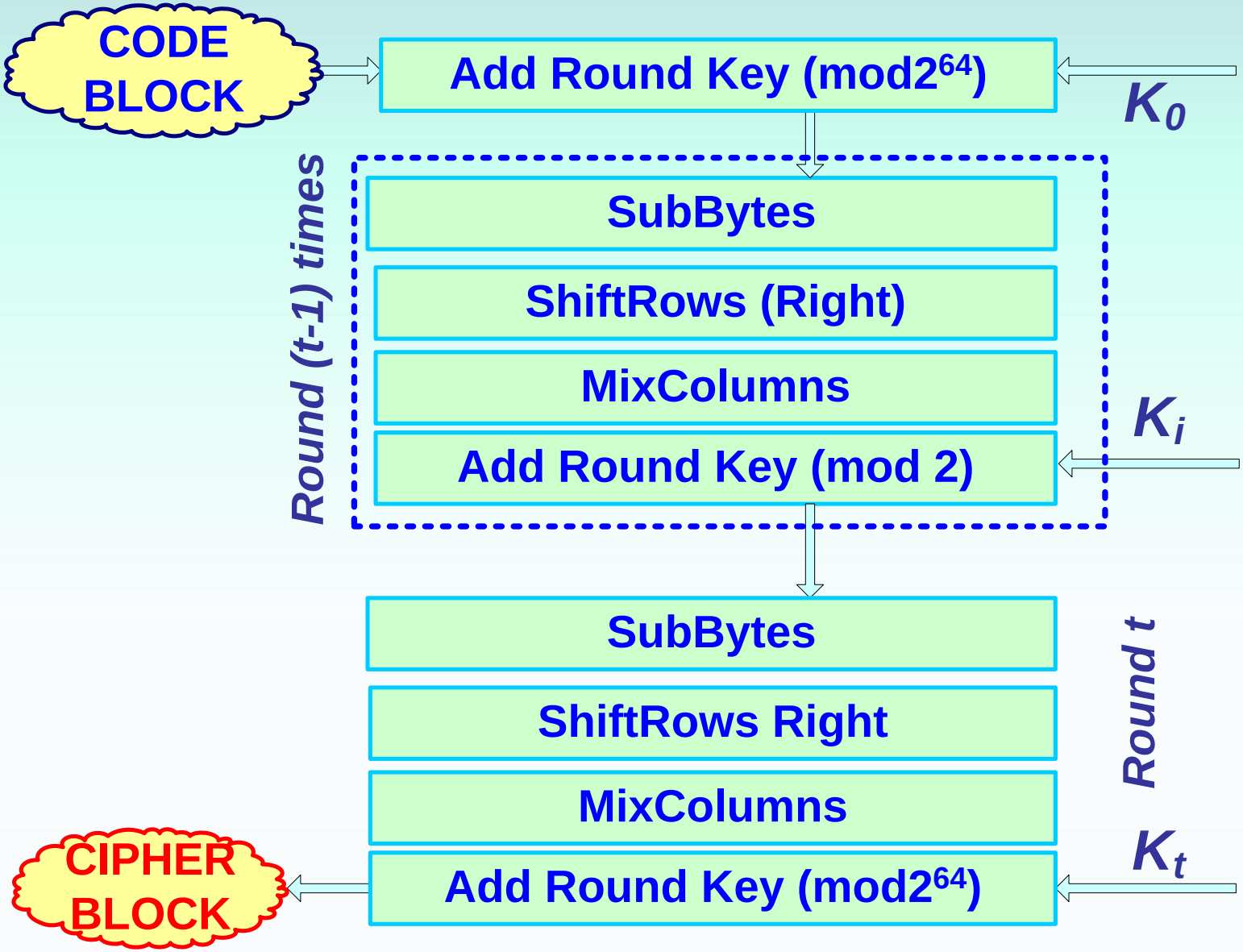
БЗ № 12–2014/633

Київ
МІНЕКОНОМРОЗВИТКУ УКРАЇНИ
2016

Стандарт основан на AES и поддерживает размеры ключей и блоков до 512 бит.

Блок (бит)	Ключ (бит)	Раундов
128	128	10
	256	14
256	256	14
	512	18
512	512	18

Структурная схема стандарта «Калина»



Операции стандарта «Калина»

Add Round Key. Операция арифметического сложения (вычитания) с ключом раунда 0 и последнего (***t***-го) раунда по модулю $\mathbf{2^{64}}$.

Add Round Key. Операция сложения по модулю 2 для промежуточных раундов.

SubBytes. Подстановка каждого байта состояния на соответствующий ему байт из одной из 4-х таблиц подстановки (*S0*, *S1*, *S2*, *S3*) каждая размером 256 байт.

ShiftRows. Циклический сдвиг байтов строк состояния. Величина сдвига определяется номером строки и величины блока.

Операции стандарта «Калина»

Mix Columns. Преобразование матрицы состояния путем умножения столбцов матрицы состояния на матрицу ***V*** в конечном поле $GF(2^8)$ по модулю неприводимого полинома

$$x^8 + x^4 + x^3 + x^2 + 1.$$

Элементы матрицы ***V*** задаются с помощью сдвигов определённых стандартом констант .

Генерация раундовых ключей из секретного (мастер) ключа выполняется с помощью аналогичных преобразований

Криптостойкость стандарта «Калина»

Различные виды дифференциального криптоанализа:

- **Блок 128 бит**

Вычислительная сложность взлома не менее 2^{55} эквивалентных операций шифрования.

- **Блок 256 бит**

Вычислительная сложность взлома не менее $2^{61} + 2^{66}$ байт памяти.

- **Блок 512 бит**

Вычислительная сложность взлома не менее $2^{60} + 2^{66}$ байт памяти.

Атака грубой силы неосуществима.

«Калина» обеспечивает

- Высокий и сверхвысокий уровень криптостойкости с запасом на появление новых атак и усовершенствования криптоаналитических комплексов в течение длительного времени.
- Высокую скорость программной реализации на современных вычислительных платформах.
- Более высокую или сравнительную эффективность относительно мировых решений.
- Наличие режимов работы, необходимых для эффективной реализации современных средств криптографической защиты.
- Возможность интеграции двух национальных стандартов в едином комплексе криптографической защиты.

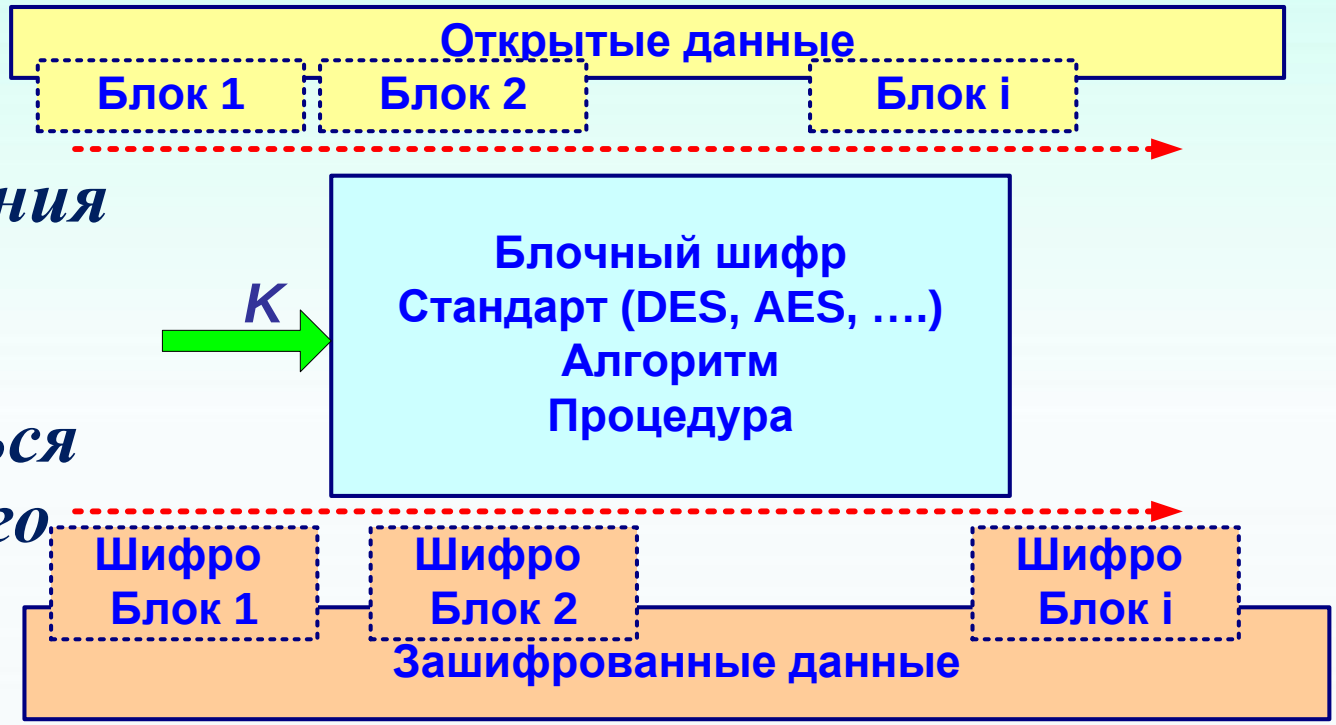
Режимы блочного шифрования

1. ECB – Electronic Codebook.
2. CBC – Cipher Block Chaining
3. PCBC – Propagating CBCCFB
4. CFB - Cipher Feedback
5. OFB – Output Feedback
6. CTR – Counter Mode
7. GCM – Galois|Counter Mode

Режимы блочного шифрования

Режим - метод применения блочного шифра (стандарта, алгоритма), позволяющий преобразовать последовательность блоков открытых данных в последовательность блоков зашифрованных данных.

Важно:
для шифрования одного блока могут использоваться данные другого блока.

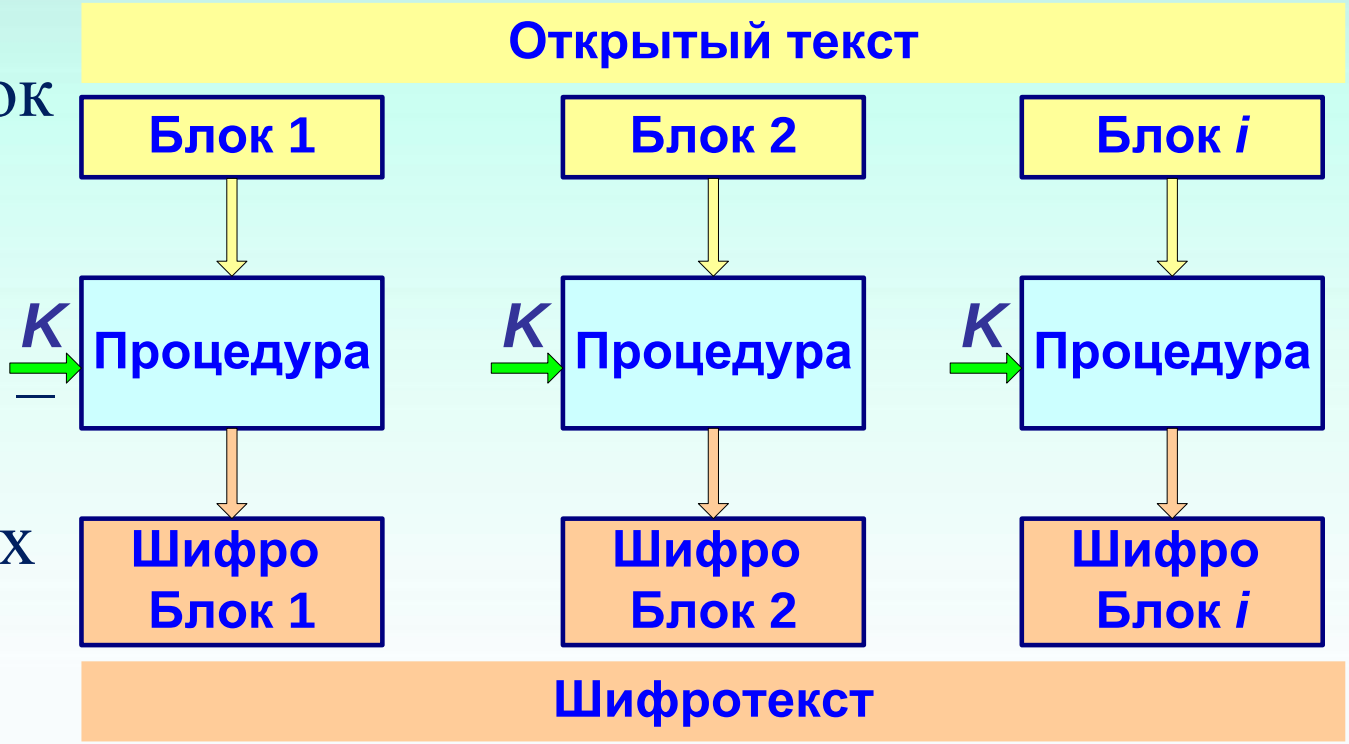


$$P \rightarrow P_1, P_2, P_3, \ldots, P_n \rightarrow C_1, C_2, C_3, \ldots, C_n \rightarrow C$$

Режим ECB – Electronic Codebook.

Режим простой замены.

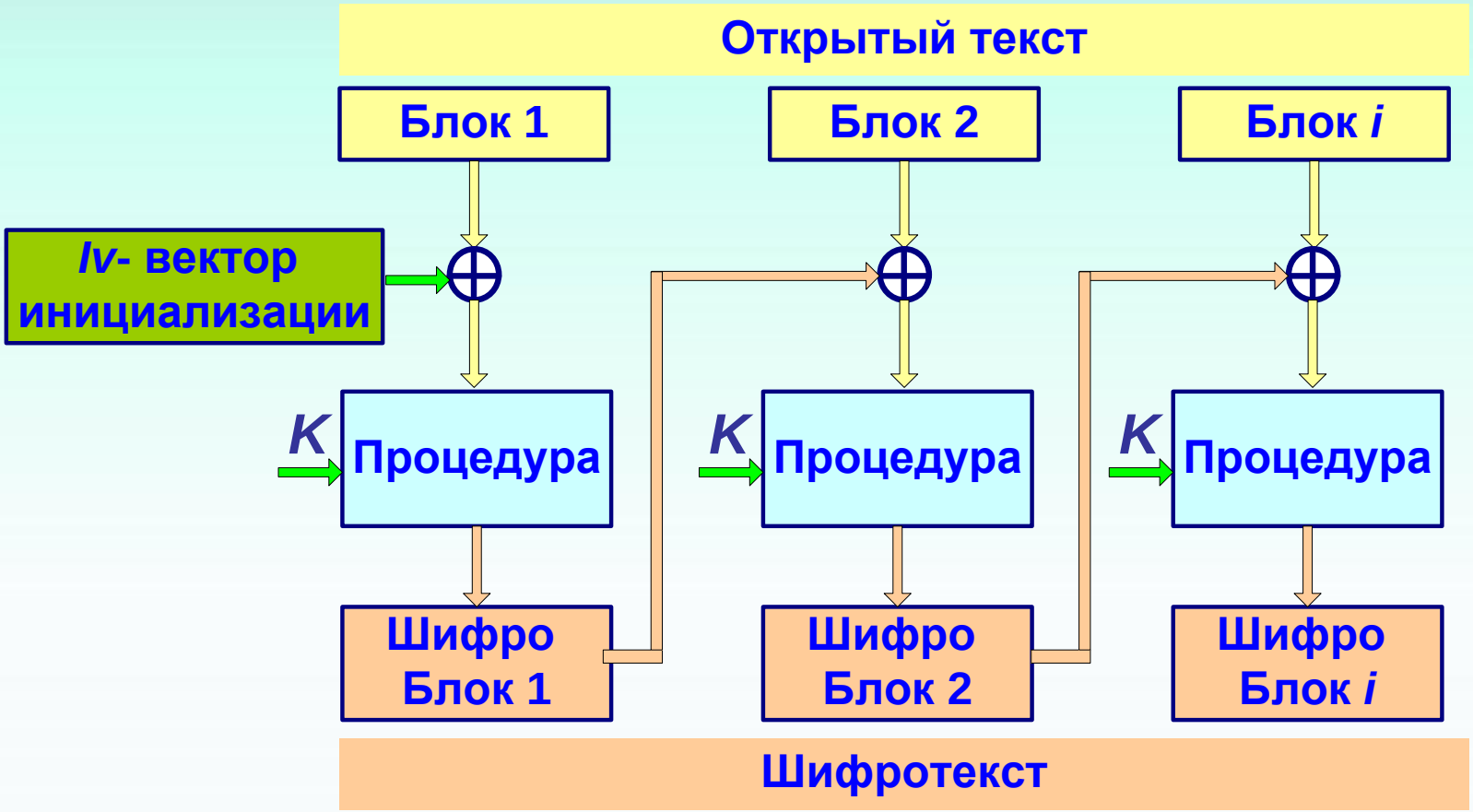
Каждый блок шифруется независимо друг от друга.
!!Недостаток – сохранение статистических особенностей.



Шифрование: $C_i = E(P_i, K)$,
Дешифрование: $P_i = D(C_i, K)$

Режим CBC – Cipher Block Chaining.

Режим сцепления блоков (замена с зацеплением).

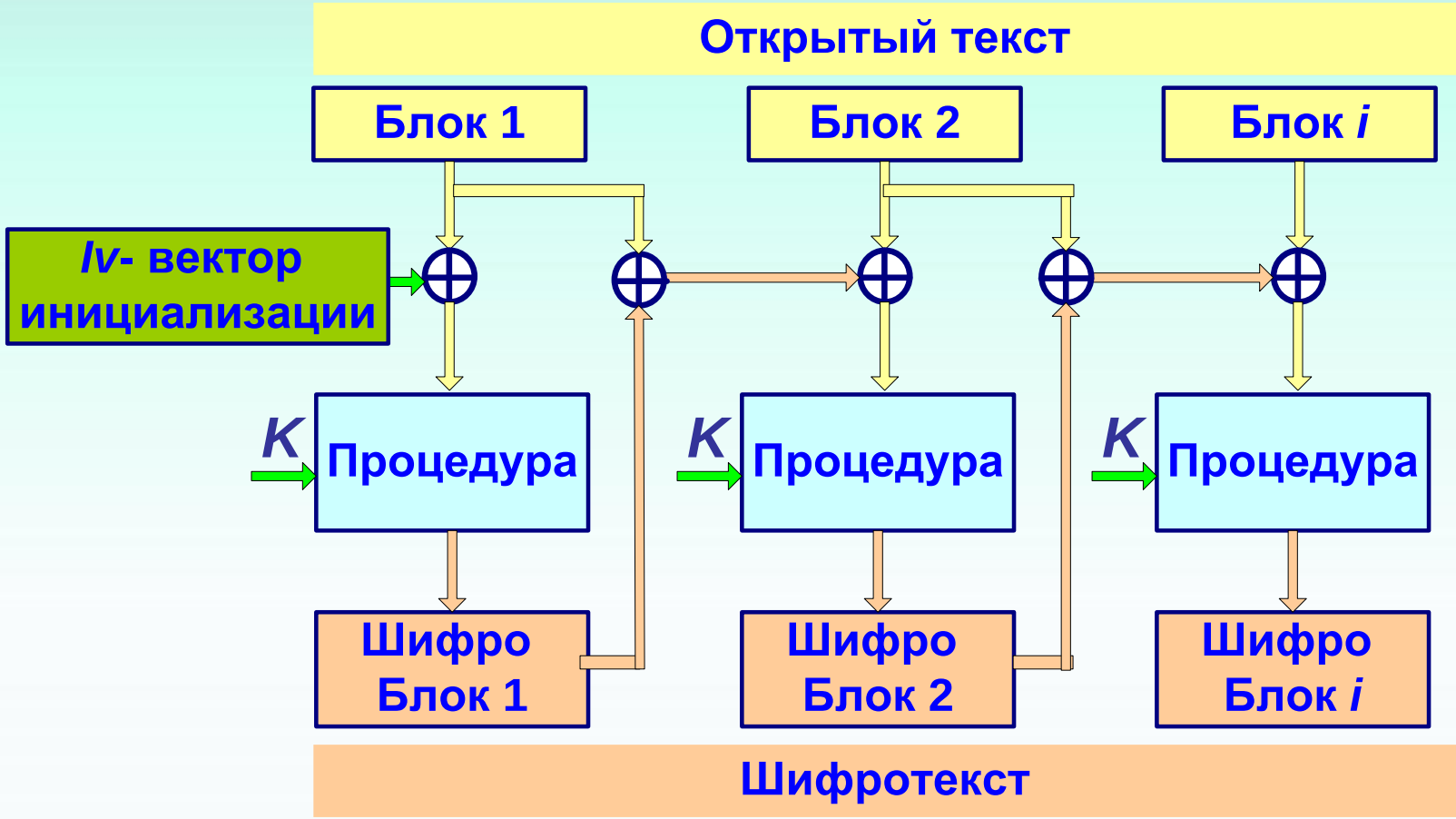


Шифрование: $C_o = I_v, C_i = E(P_i \oplus C_{i-1}, K)$

Дешифрование: $C_o = I_v,\ P_i = C_{i-1} \oplus D(C_i, K)$

Режим PCBC – Propagation CBC

Режим распространяющегося сцепления блоков.

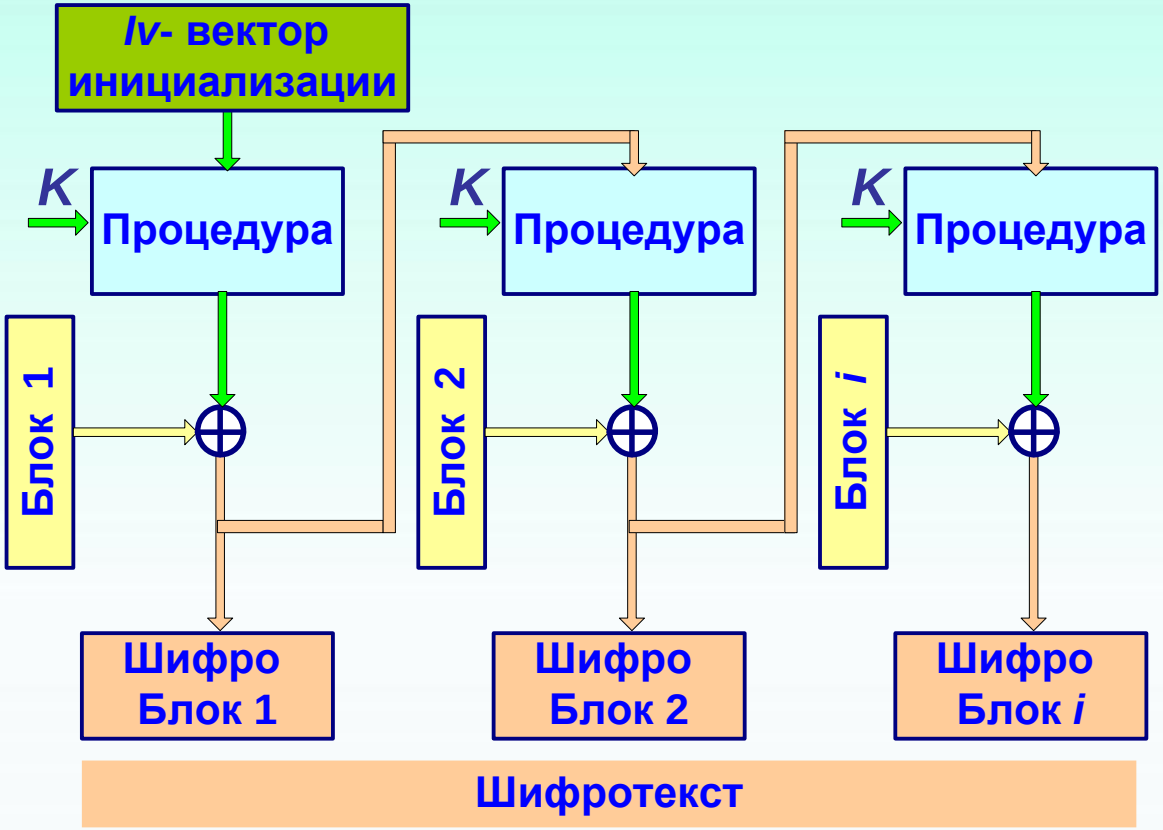


Шифр: $C_1 = E(P_1 \oplus I_v, K)$, $C_i = E(P_i \oplus P_{i-1} \oplus C_{i-1}, K)$

Дешифр: $C_o = I_v$, $P_i = P_{i-1} \oplus C_{i-1} \oplus D(C_i, K)$

Режим CFB - Cipher Feedback

Режим обратной связи по шифротексту (гаммирование с обратной связью)



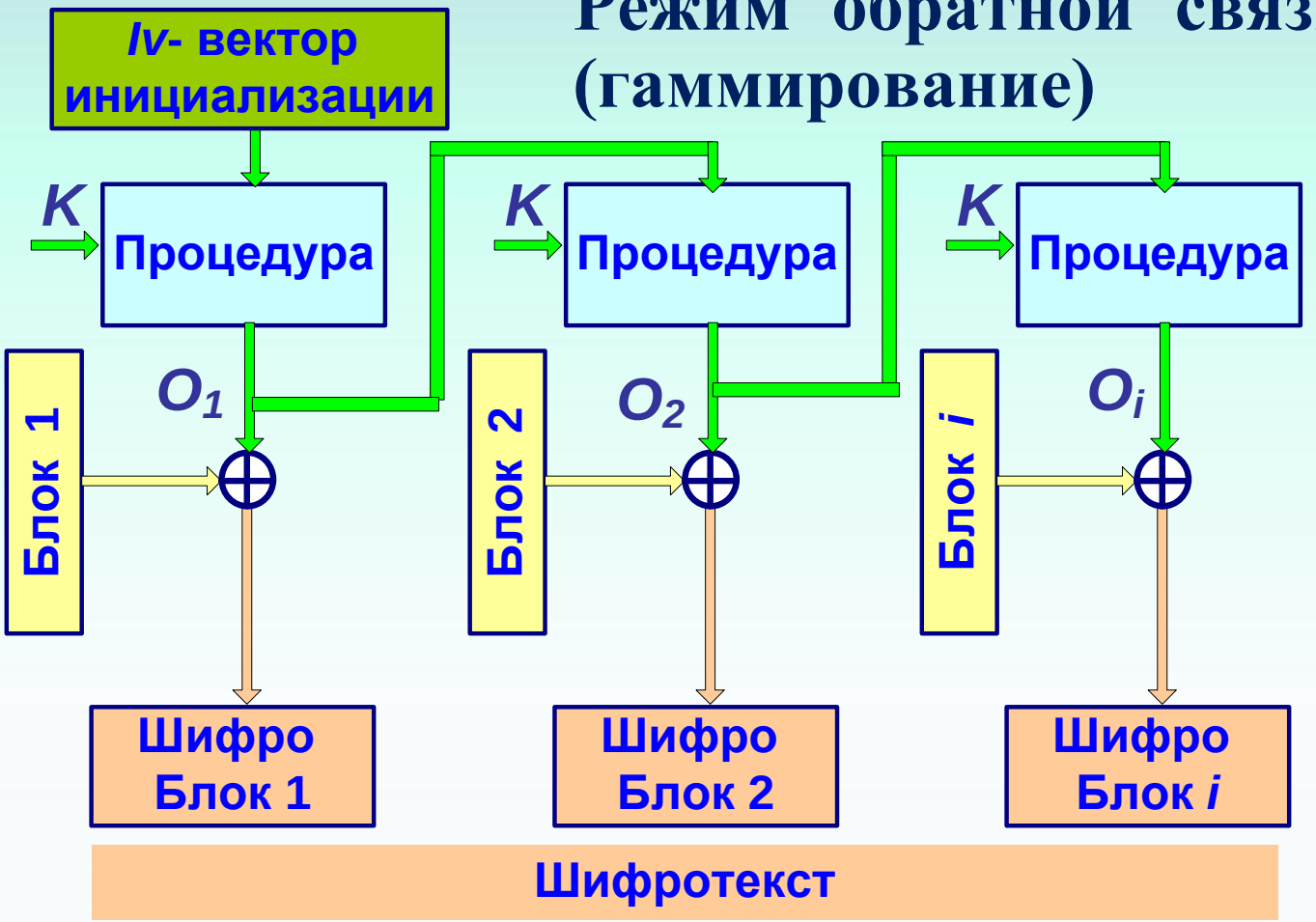
Блоки отрытых данных смешиваются с блоками зашифрованных данных. Криптостойкость = криптостой-кости E

Шифр: $C_o = I_v, C_i = E(C_{i-1}, K) \oplus P_i$

Дешифр: $P_i = E(C_{i-1}, K) \oplus C_i$

Режим OFB – Output Feedback

Режим обратной связи по выходу (гаммирование)



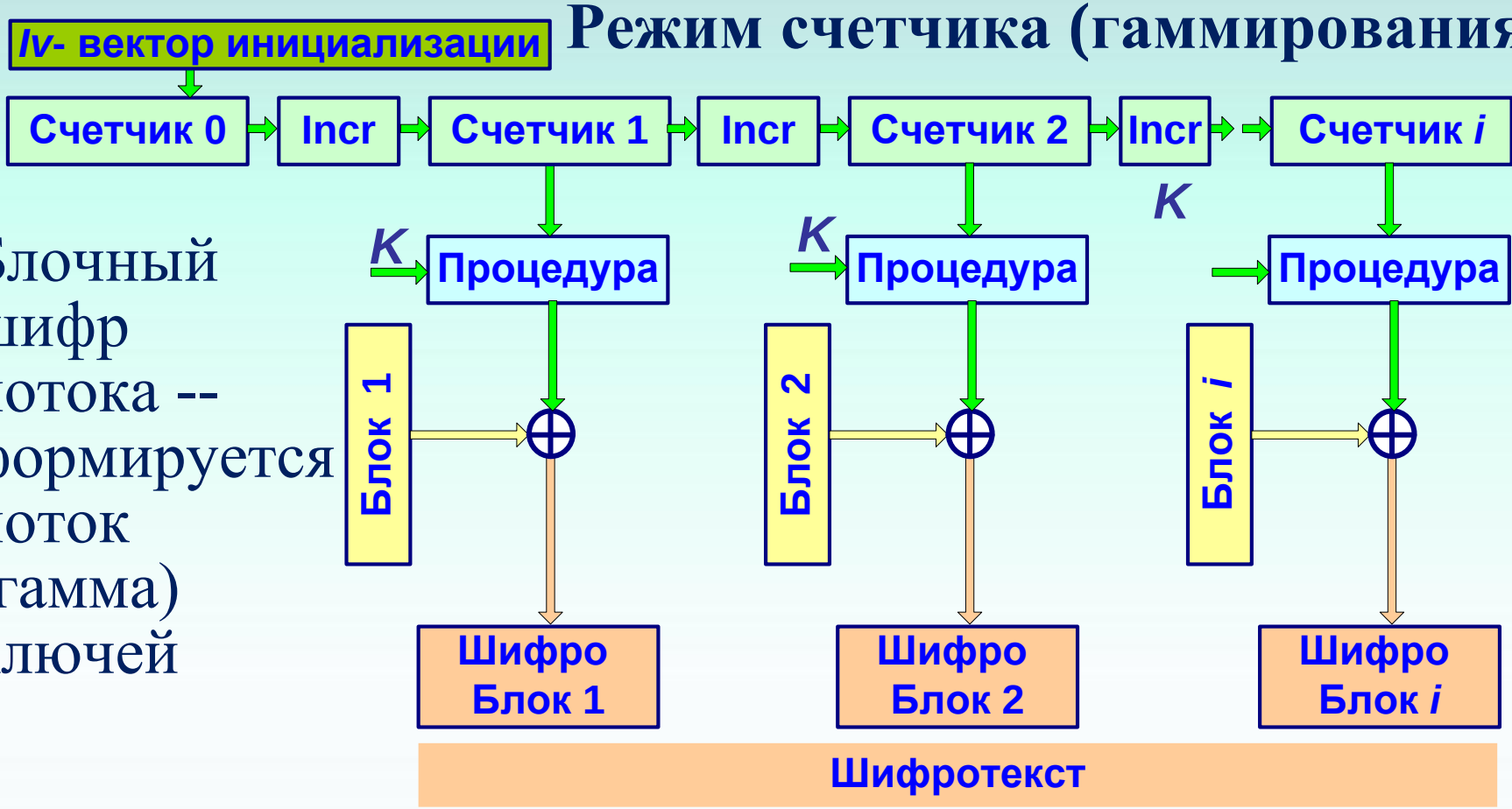
!!! Блочный шифр потока -- формируется поток (гамма) ключей

Шифр: $C_o = I_v, O_i = E(O_{i-1}, K), C_i = O_i \oplus P_i$

Дешифр: $P_i = O_i \oplus C_i$

Режим CTR – Counter Mode

Режим счетчика (гаммирования)



Блочный шифр потока -- формируется поток (гамма) ключей

Счетчик: $Ctr_0 = I_v, Ctr_i \mathrel{+}= Incr$

Шифр: $C_i = P_i \oplus E(Ctr_i), Ctr_0 = I_v, Ctr_i \mathrel{+}= Incr$

Дешифр: $P_i = C_i \oplus E(Ctr_i)$

Режимы работы

Вектор инициализации I_v .

В таких режимах CBC, CFB и OFB на вход подаётся вектор инициализации I_v.

Причём Алиса и Боб в начале сеанса связи должны иметь один и тот же I_v. Может быть и не секретным.

Важно:

- в режимах CBC и CFB I_v должно быть непредсказуемым,
- в режиме OFB — уникальным.

Выбор режима. Зависит от поставленной цели и требований.

Обычный открытый текст CBC, CFB или OFB.

Для шифрования файлов CBC.

Выбор - компромисс между эффективностью и производительностью.

Режимы работы «Калина»

		Название	Услуга
1	ECB	Простая замена	Конфиденциальность
2	CTR	Гаммирование	Конфиденциальность
3	CFB	Гаммирование с обратной связью	Конфиденциальность
4	CBC	Сцепление шифроблоков	Конфиденциальность
5	OFB	Гаммирование с обратной связью шифроблоков	Конфиденциальность
6	GCM \ GMAC	Избранное гаммирование с быстрой генерацией имитовставки	Конфиденциальность Целостность

Вопросы:

- Укажите особенности организации шифрования и основные операции стандарта «Калина».
- Охарактеризуйте стандарт «Калина» и определите его режимы работы.
- Охарактеризуйте режим **ECB** работы блочного шифра.
- Охарактеризуйте режим **CBC** работы блочного шифра.
- Охарактеризуйте режим **OFB** работы блочного шифра.
- Охарактеризуйте режим **CFB** работы блочного шифра.
- Охарактеризуйте режим **CTR** работы блочного шифра.

ЛИТЕРАТУРА

ДСТУ 7624:2014 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення.

Wiki

https://uk.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BB%D0%B8%D0%BD%D0%B0_(%D1%88%D0%B8%D1%84%D1%80)

ЛИТЕРАТУРА

Нечаев В.И. Элементы криптографии (Основы теории защиты информации).- Учеб. пособие. – М.:, ВШ., 1999.- 109 с.

Введение в криптографию. **Под общ. ред. В.В.Ященко.** – 4-е изд., доп. М.: МЦНМО, 2012 – 348 с. ISBN 978-5-4439-0026-1

ЛИТЕРАТУРА

Венбо Мао. Современная криптография: теория и практика.—М.: Издательский дом «Вильямс», 2005.—768 с.: ил. ISSN 5-8459-0847-7 (рус.)

Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на Си. – Москва: Вильямс, 2016. 1024 с.

ЛИТЕРАТУРА

Francisco Rodriguez-Henriquez, N.A. Saqib, A. Diaz-Perez, Cetin Kaya Koc.

Cryptographic Algorithms on Reconfigurable Hardware. - Springer, 2006.

A. Menezes, P. van Oorschot, S. Vanstone.

Handbook of Applied Cryptography.- CRC Press, 1996.

END # 13