Часть IV. Режимы использования блочных шифров

Блочные шифры оперируют многими блоками открытых данных и шифртекста. Открытый текст

$$P = P_1\, P_2\, \ldots\, P_m$$

разбивается на блоки P_i одинаковой длины (длина блока обычно составляет 64 или 128 битов, иногда длиннее) и преобразуется в шифртекст

$$C = C_1\, C_2\, \ldots\, C_m,$$

также разбитый на блоки C_i. Блок P_i и соответствующий ему блок C_i обычно имеют одинаковую длину. Последний блок P_m в сообщении P может быть неполным (укороченным). Неполный блок обычно дополняют одним из способов: до требуемой длины n: 1) добавляется битовая единица и необходимое число битовых нулей; 2) добавляется необходимое число случайных байтов, но в последнем байте записывается число добавленных байтов.

Чтобы метод работал корректно, следует дополнять каждое сообщение, даже если открытый текст заканчивается на границе блока. Отметим, что имеются альтернативные варианты шифрования, называемые *похищением*, или *заимствованием текста* ($ciphertext\ stealing$), оперирующие с неполным последним блоком, при которых длины открытого текста P и шифртекста C совпадают.

Далее $\mathcal{E}_k$ обозначает n-битовую функцию зашифрования, а $\mathcal{D}_k$ – обратную к ней функцию расшифрования; P_i – n-битовый блок открытых данных, а C_i – соответствующий ему блок шифртекста. Задание данного раздела предусматривает зашифрование открытого сообщения с присоединенной к нему цифровой подписью в одном из предлагаемых ниже режимов 1-14.

1. ECB

Режим *электронной кодовой книги* – ECB ($Electronic\ Code\ Book$). В ГОСТ 28147-89 этот режим называется *режимом простой замены*.

Режим ECB – простейший режим шифрования. Все блоки открытого текста шифруются независимо друг от друга. Уравнения зашифрования и расшифрования имеют вид (см. рис. 1):

$$C_i := \mathcal{E}_k(P_i), \quad i = 1,2,\ldots,m;$$
$$P_i := \mathcal{D}_k(C_i), \quad i = 1,2,\ldots,m.$$

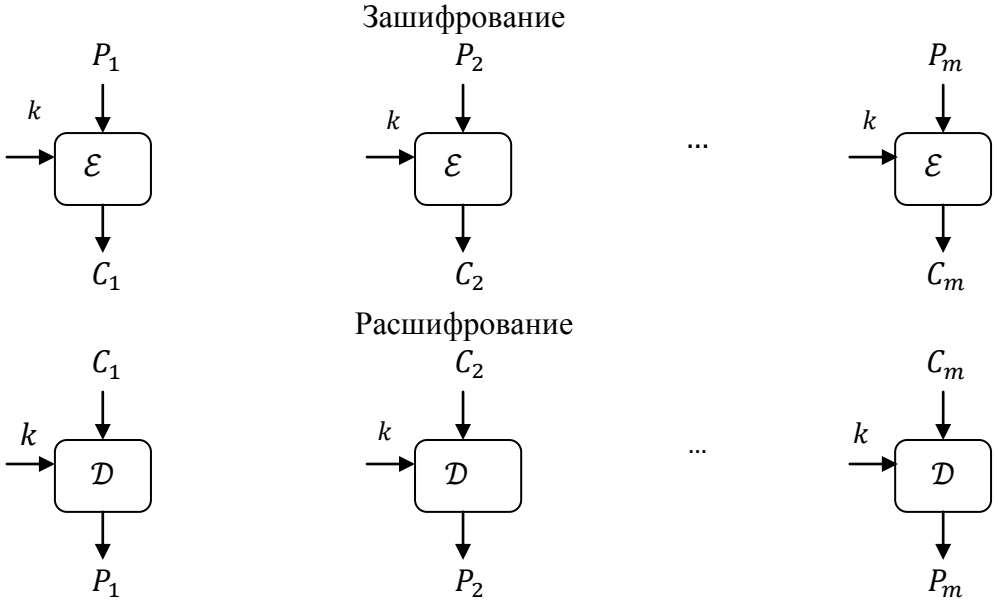


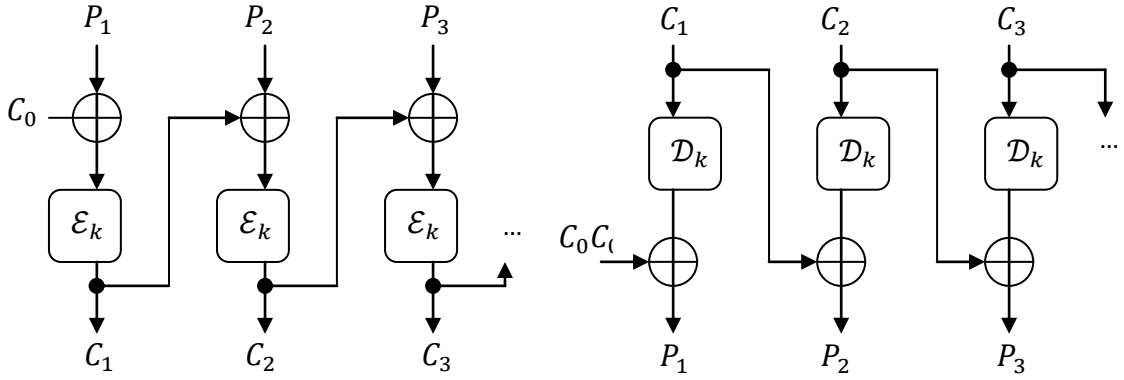
Рис. 1. *Режим электронной кодовой книги EBC*

2. CBC

Режим *сцепления блоков шифртекста – CBC* ($Cipher\ Block\ Chaining$). Уравнения зашифрования и расшифрования имеют вид (см. рис. 2):

$$C_i := \mathcal{E}_k(P_i \oplus C_{i-1}), i = 1,2,\dots,m;$$
$$P_i := \mathcal{D}_k(C_i) \oplus C_{i-1}, i = 1,2,\dots,m.$$

Здесь C_0 – блок, значение которого известно как отправителю, так и получателю сообщения. Блок C_0 называют *вектором инициализации* (*iv – initial vector*, русский термин – *синхропосылка*). Рекомендуется для каждого сообщения выбирать уникальный вектор инициализации (используя, например, метку времени) и передавать его получателю в зашифрованном виде.



(*а*) Зашифрование (*б*) Расшифрование

Рис. 2. *Режим сцепления блоков шифртекста CBC*

3. CFB

Режим ***обратной связи по шифртексту*** *– CFB* ($Cipher\ Feed\ Back$). В ГОСТ 28147-89 аналогичный режим называется *режимом гаммирования с обратной связью*. Уравнения зашифрования и расшифрования имеют вид (см. рис.3):

$$C_i := P_i \oplus \mathcal{E}_k(C_{i-1}), i = 1,2,\dots,m;$$
$$P_i := C_i \oplus \mathcal{E}_k(C_{i-1}), i = 1,2,\dots,m.$$

Значение C_0 задается при помощи вектора инициализации и передается получателю в открытом виде.

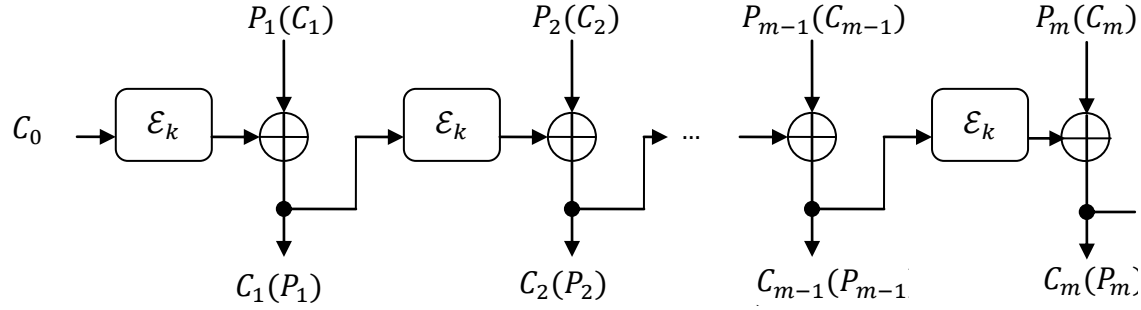


Рис. 3. *Режим обратной связи по шифртексту CFB*

4. OFB

Режим ***обратной связи по выходу*** *– OFB* ($Output\ Feed\ Back$). Уравнения зашифрования и расшифрования имеют вид (см. рис.4а):

$$C_i := P_i \oplus \gamma_i, i = 1,2,\dots,m;$$
$$P_i := C_i \oplus \gamma_i, i = 1,2,\dots,m.$$

Последовательность γ_1, γ_2, …, называемая *гаммой* шифра, вырабатывается по правилу:

$$\gamma_i = \mathcal{E}_k\,(\gamma_{i-1}), i = 1,2, \ldots.$$

Значение γ_0, задаваемое *вектором инициализации* (*синхропосылкой*), должно быть уникальным для каждого сообщения, но сохранять его в тайне не обязательно.

5. Counter

Режим ***счетчика*** – $Counter$. В ГОСТ 28147-89 ему соответствует *режим гаммирования.* Уравнения зашифрования и расшифрования имеют вид (см. рис.4б):

$$C_i := P_i \oplus \gamma_i, i = 1,2, \ldots, m;$$
$$P_i := C_i \oplus \gamma_i, i = 1,2, \ldots, m.$$

Гамма шифра γ_1, γ_2, … вырабатывается по правилу:

$$\gamma_i = \mathcal{E}_k(s_i),$$

где s_i – некоторая последовательность чисел, определяемая формулой $s_i = s_{i-1} + 1$ либо каким-либо другим способом.

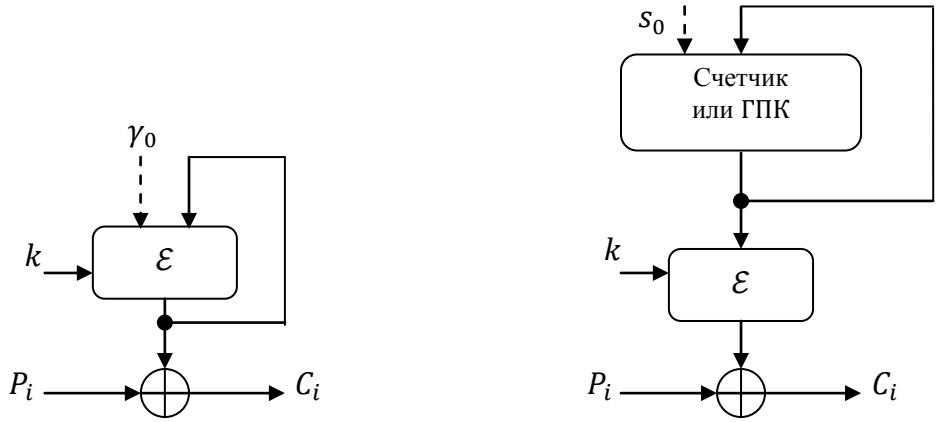


Рис. 4. (*а*) *Зашифрование в режиме* OFB; (*б*) *зашифрование в режиме счетчика* (ГПК – *генератор псевдослучайных кодов*). *Расшифрование осуществляется аналогично*

6. PBC

Режим ***сцепления блоков открытого текста*** – PBC ($Plaintext\ Block\ Chaining$) – является обратным к режиму CBC. Уравнения зашифрования и расшифрования имеют вид (см. рис .5):

$$C_i := \mathcal{E}_k(P_i) \oplus P_{i-1}, i = 1,2, \ldots, m;$$
$$P_i := \mathcal{D}_k(C_i \oplus P_{i-1}), i = 1,2, \ldots, m.$$

Значение P_0 задается *вектором инициализации* (*синхропосылкой*).

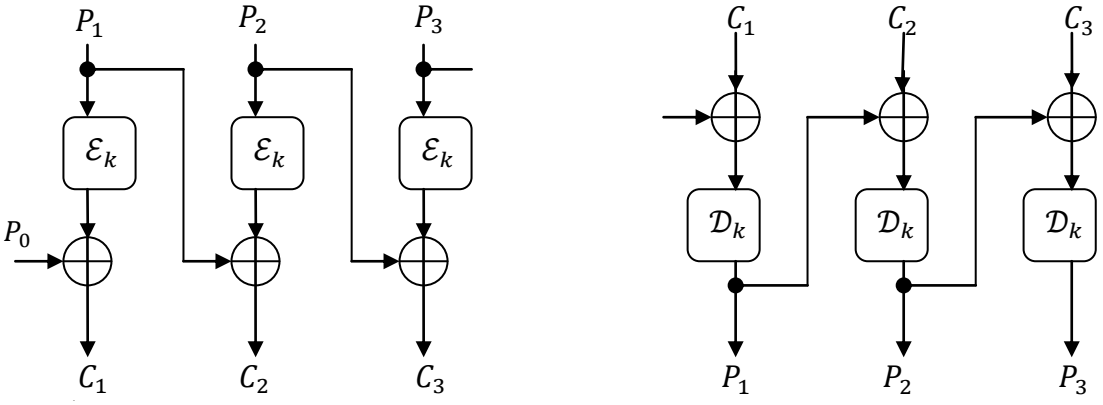


Рис. 5. *Режим сцепления блоков открытого текста PBC*

7. PFB

Режим ***обратной связи по открытому тексту*** – PFB ($Plaintext\ Feed\ Back$) – является обратным к режиму CFB. Уравнения зашифрования и расшифрования имеют вид (см. рис. 6):

$$C_i := P_i \oplus \mathcal{E}_k(P_{i-1}), i = 1,2,\dots,m;$$
$$P_i := C_i \oplus \mathcal{E}_k(P_{i-1}), i = 1,2,\dots,m.$$

Значение P_0 задается вектором инициализации (синхропосылкой).

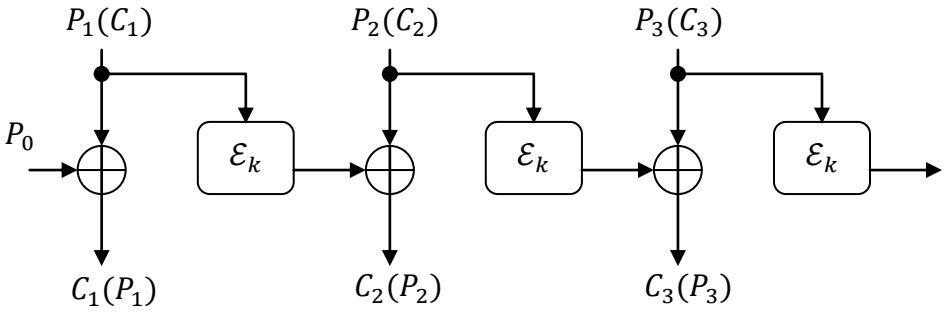


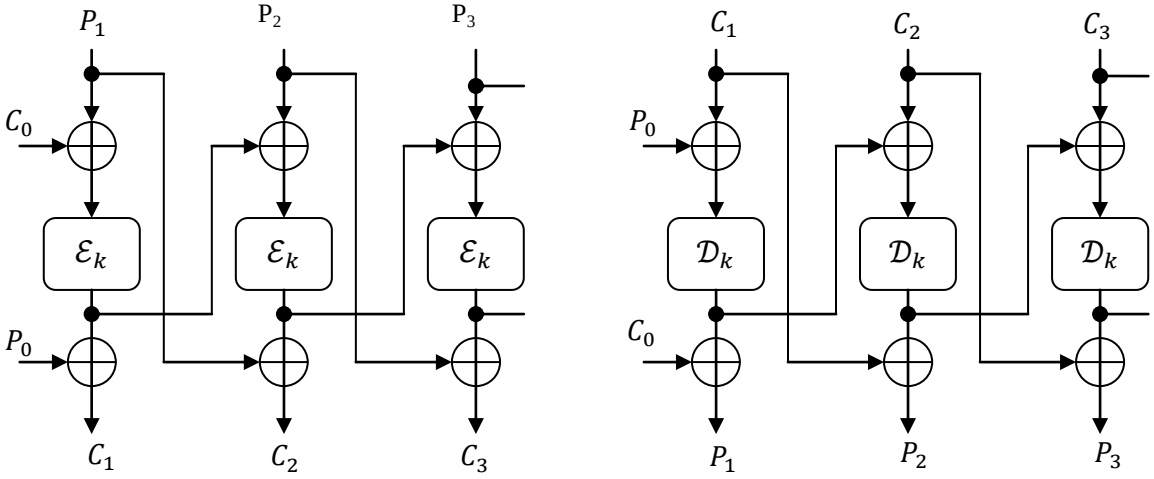
Рис. 6. *Режим обратной связи по открытому тексту PFB*

8. Модификация CBC

Режим ***усиленного сцепления блоков шифртекста*** – модификация режима CBC. Уравнения зашифрования и расшифрования имеют вид

$$C_i := P_{i-1} \oplus \mathcal{E}_k(P_i \oplus C_{i-1}), i = 1,2,\dots,m;$$
$$P_i := C_{i-1} \oplus \mathcal{D}_k(C_i \oplus P_{i-1}), i = 1,2,\dots,m.$$

Значения C_0 и P_0 задаются *векторами инициализации* (*синхропосылками*).



(*а*) Зашифрование (*б*) Расшифрование

Рис. 7. *Режим усиленного сцепления блоков шифртекста CBC*

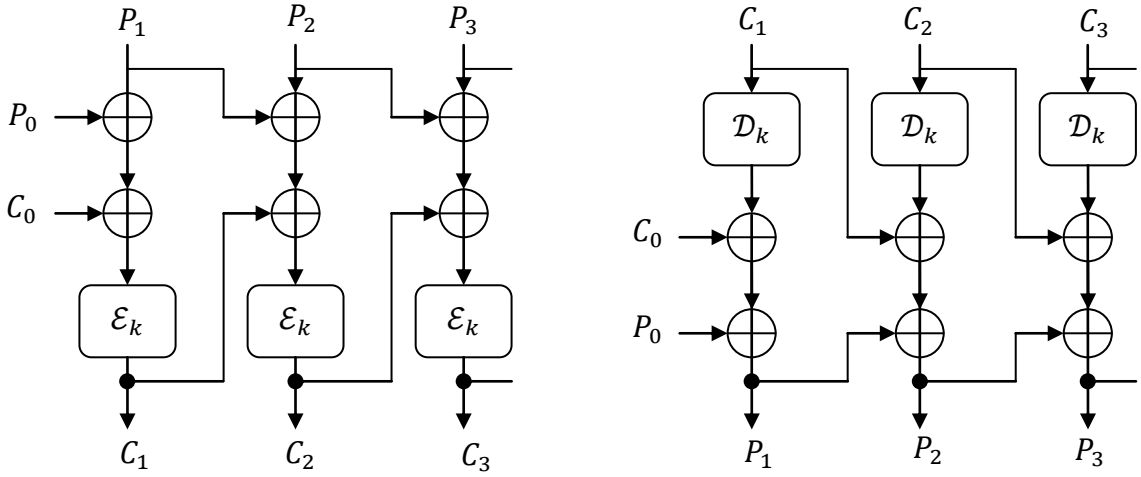
9. PCBC

Режим ***сцепления блоков шифртекста с распространением ошибки*** – $PCBC$ ($Propagating\ Cipher\ Block\ Chaining$), как и предыдущий режим, является модификацией режима CBC. Уравнения зашифрования и зашифрования имеют вид (см. рис.8):

$$C_i := \mathcal{E}_k(P_i \oplus P_{i-1} \oplus C_{i-1}), i = 1,2,\dots,m;$$

$$P_i := \mathcal{D}_k(C_i) \oplus C_{i-1} \oplus P_{i-1}, i = 1,2,\dots,m.$$

Значение $C_0 \oplus P_0$ задается *вектором инициализации*.



(*а*) Зашифрование (*б*) Расшифрование

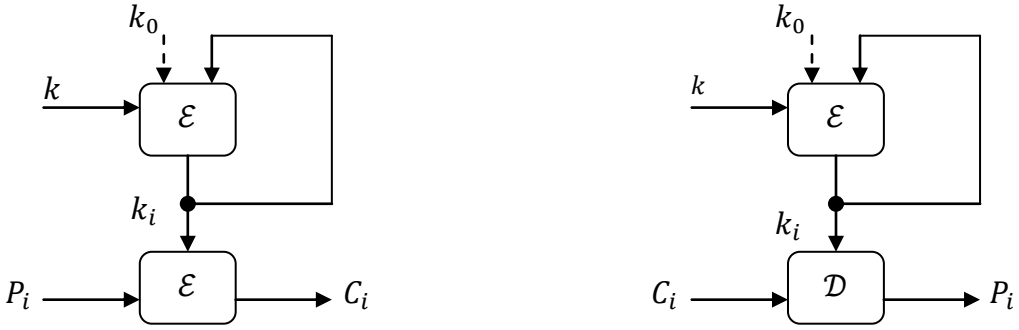
Рис. 8. *Режим сцепления блоков шифртекста с распространением ошибки* PCBC

10. OFBNLF

Режим ***нелинейной обратной связи по выходу*** – $OFBNLF$ ($Output\ Feed\ Back\ with\ Nonlinear\ Function$) – смешанный вариант режимов OFB и ECB, где ключ изменяется в каждом блоке. Уравнения зашифрования и расшифрования имеют вид (см. рис. 9):

$$C_i := E_{k_i}(P_i), k_i = \mathcal{E}_k(k_{i-1}), i = 1,2,\dots,m;$$
$$P_i := D_{k_i}(C_i), k_i = \mathcal{E}_k(k_{i-1}), i = 1,2,\dots,m.$$

Значение k_0 задается *вектором инициализации* (*синхропосылкой*).



(*а*) Зашифрование (*б*) Расшифрование

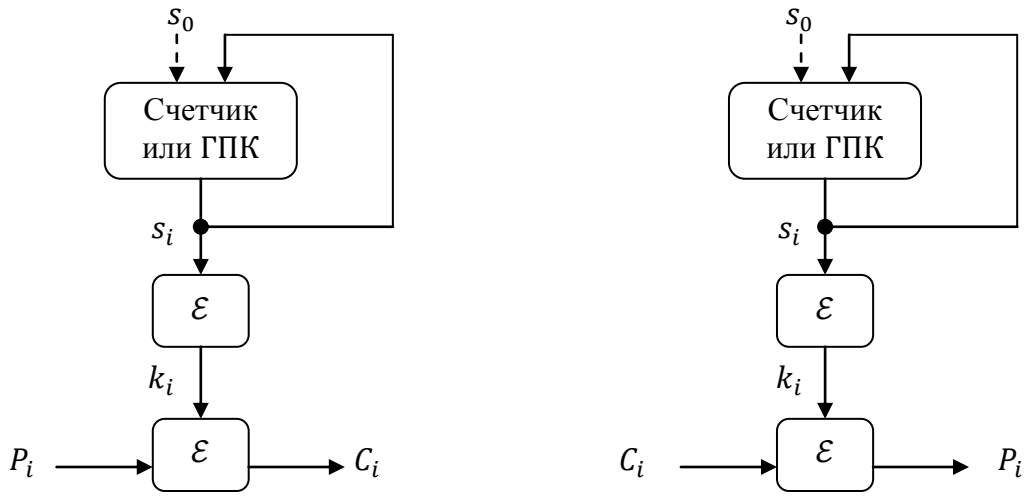
Рис. 9. *Режим нелинейной обратной связи по выходу* $OFBNLF$

11. CNLF

Режим ***счетчика с нелинейной функцией*** – $CNLF$ ($Counter\ with\ Nonlinear\ Function$). Уравнения зашифрования и расшифрования имеют вид (см. рис. 10):

$$C_i := \mathcal{E}_{k_i}(P_i), k_i = \mathcal{E}_k(s_i), i = 1,2,\dots,m;$$
$$P_i := \mathcal{D}_{k_i}(C_i), k_i = \mathcal{E}_k(s_i), i = 1,2,\dots,m.$$

Последовательность $s_1, s_2, \dots$ вырабатывается, например, по правилу $s_i = s_{i-1} + 1$ либо каким-нибудь другим способом (например, с использованием ГПК – генератора псевдослучайных кодов), исходя из начального значения s_0, заданного вектором инициализации (синхропосылкой).



(*а*) Зашифрование (*б*) Расшифрование

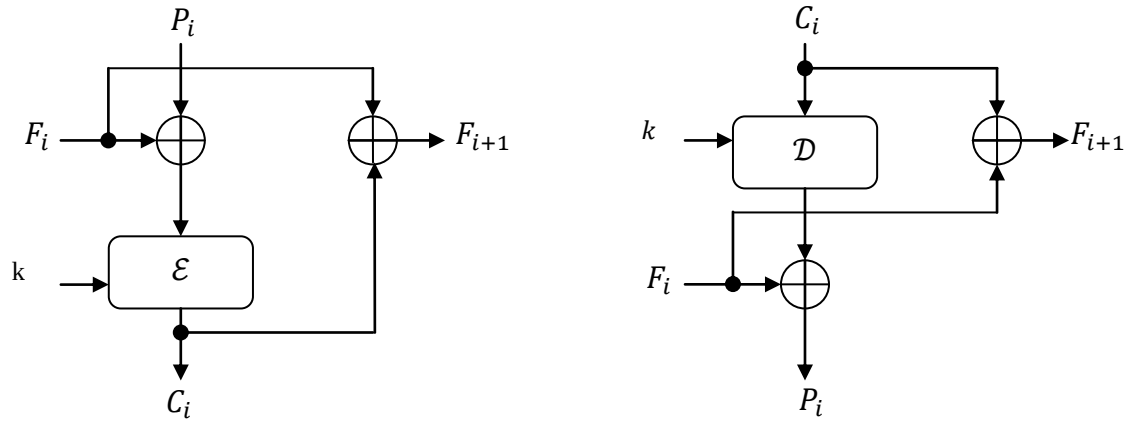
Рис. 10. *Режим счетчика с нелинейной функцией CNLF*

12. BC

Режим ***сцепления блоков*** – BC $(Block\ Chaining\ mode)$. Уравнения зашифрования и расшифрования имеют вид (см. рис. 11):

$$C_i := \mathcal{E}_k(P_i \oplus F_i), i = 1,2, \dots, m;$$
$$P_i := \mathcal{D}_k(C_i) \oplus F_i, i = 1,2, \dots, m.$$

Значение F_1 задается *вектором инициализации*, $F_i = F_{i-1} \oplus C_{i-1}$ при $i \geq 2$.



(*а*) Зашифрование (*б*) Расшифрование

Рис. 11. *Режим сцепления блоков BC mode*

13. CTS

Режим ***заимствования шифрованного текста – CTS*** $(Cipher\ Text\ Stealing)$ – модификация режима CBC, допускающая обработку текста любой длины и генерирующая шифртекст точно такой же длины.

Пусть $P = P_1P_2 \dots P_{m-1}P_m$ – открытый текст, разбитый на блоки P_i, $1 \leq i \leq m$, где P_m – неполный блок, имеющий длину q битов вместо положенной длины n битов для полного блока, $q < n$. Шифртекст $C = C_1C_2 \dots C_{m-1}C_m$, где C_m – неполный блок длины q, получается по схеме (см. рис.12):

1) первые $m - 2$ блоков P_i шифруются с помощью стандартной техники CBC:

$$C_i := \mathcal{E}_k(P_i \oplus C_{i-1}), i = 1, \dots, m - 2;$$

2) шифруется побитовая сумма блоков P_{m-1} и C_{m-2}:

$$X := \mathcal{E}_k(P_{m-1} \oplus C_{m-2});$$

в блоке X выбираются, которые первые q битов образуют неполный блок C_m;

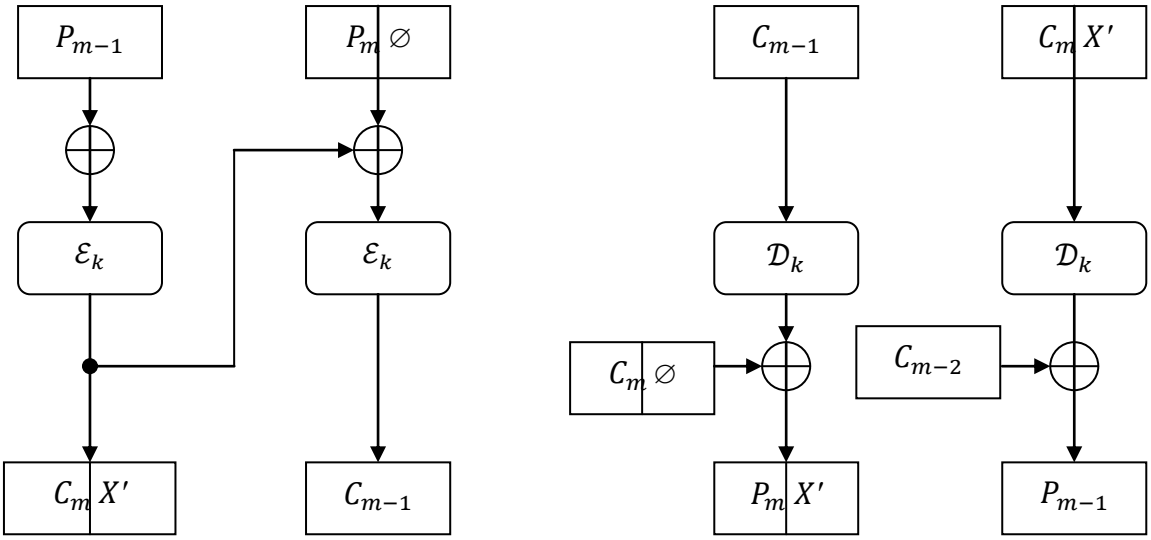
3) блок P_m дополняется нулями до полного блока и суммируется с блоком X; результат шифруется, что дает блок C_{m-1}:

$$C_{m-1} := \mathcal{E}_k\ ((P_m\ ||\ 0\ \ldots 0) \oplus X).$$

Расшифрование выполняется по схеме:

1) $P_i := \mathcal{D}_k(C_i) \oplus C_{i-1}, i = 1, \ldots, m-2;$
2) $X := \mathcal{D}_k(C_{m-1}) \oplus (C_m||0);$
3) P_m образуют первые q битов блока X;
4) $P_{m-1} := \mathcal{D}_k\ (C_m||X') \oplus\ C_{m-2},$

где X' – блок, образованный последними $n-q$ битами блока X.



(*а*) Зашифрование (*б*) Расшифрование

Рис. 12. *Режим CTS* (*зашифрование и расшифрование двух последних блоков; начальные блоки шифруются в режим CBC*)

14. Вероятностное шифрование

Вероятностное шифрование. Основным недостатком режима EBC является тот факт, что одинаковые блоки шифруются одинаково. Чтобы устранить этот недостаток и повысить стойкость шифрования, можно использовать вероятностное шифрование, суть которого заключается в подмешивании случайных данных к шифруемому сообщению.

Пусть $\mathcal{E}_K^{(t)}$ обозначает некоторую функцию шифрования n-битового блока данных под управлением ключа K, $\mathcal{D}_K^{(t)}$ – обратную функцию, R – r-битовый случайный (псевдослучайный) блок, генерируемый датчиком случайных чисел ДСЧ, P – s-битовый блок шифруемых данных, C –
$(r+s)$-битовый блок шифртекста, результат зашифрования блока P, $(R,P) \equiv R||P$ – конкатенацию блоков R и P. Некоторые варианты вероятностного шифрования представлены на рис.13 и 14.

В первом варианте блок P следующим образом преобразуется в блок C шифртекста:

$$T :=\ E_K^{(s)}\ (\text{P});\ C :=\ E_K^{(r+s)}\ (R||T)\ .$$

Расшифрование выполняется по схеме:

$$(R,T) := \mathcal{D}_K^{(r+s)}\ (C);\ P := E_R^{(s)}(T)\ .$$

Во втором варианте блок R разбивается на два блока: r_1-битовый R_1 и r_2-битовый R_2, а блок P следующим образом преобразуется в блок C шифртекста:

$$T:= E_{R_1}^{(r_1+s)}(R_2||P);\ C:= E_K^{(r+s)}(R_1||T).$$

Расшифрование выполняется по схеме:

$$(R_1,T):= \mathcal{D}_K^{(r+s)}(C);\ (R_2,P):= \mathcal{D}_{R_1}^{(r_1+s)}(T).$$

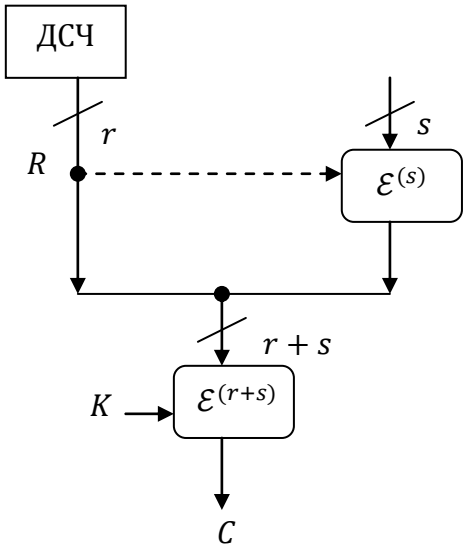


Рис. 13. *Схема с предварительным шифрованием данных под управлением случайного ключа*

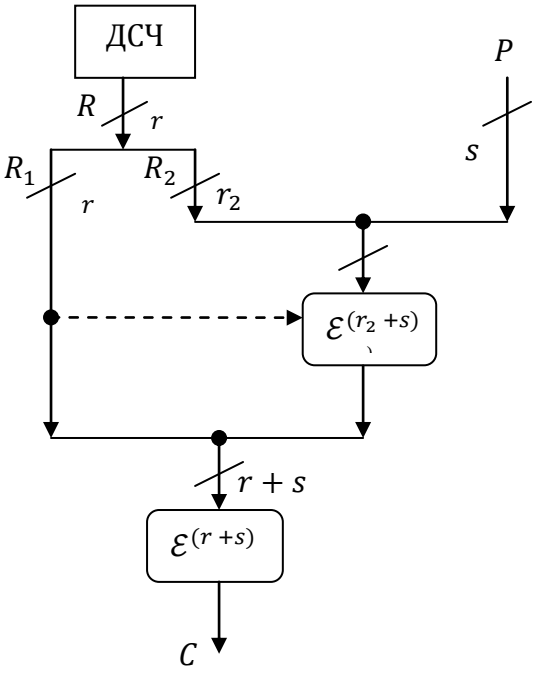


Рис. 14. *Двухступенчатое вероятностное шифрование*

Еще один вариант представлен на рис. 15.

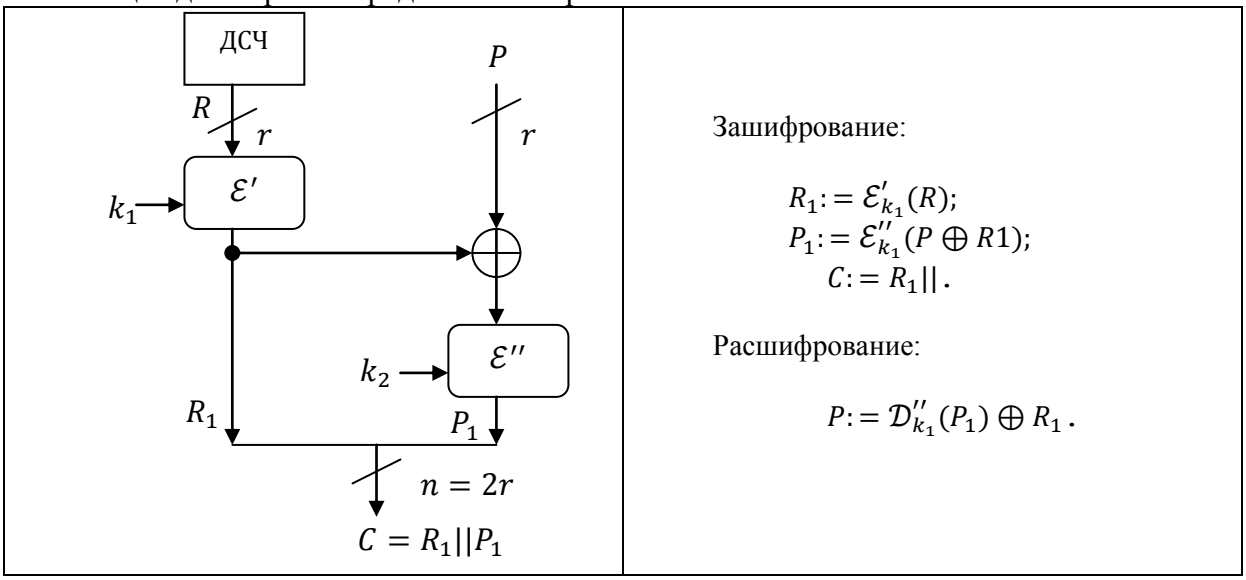


Рис. 15. *Объединение нескольких блочных алгоритмов*

К недостаткам предложенных режимов вероятностного шифрования относится увеличение размера шифртекста по сравнению с открытым текстом.