Нелинейный мир. 2013. №9. С. 647–658

УДК 511+519.719.2

ИМИТОУСТОЙЧИВАЯ ПЕРЕДАЧА ДАННЫХ В ЗАЩИЩЕННЫХ СИСТЕМАХ ОДНОНАПРАВЛЕННОЙ СВЯЗИ НА ОСНОВЕ ПОЛИНОМИАЛЬНЫХ КЛАССОВ ВЫЧЕТОВ

Д.В. Самойленко, О.А. Финько

Предложена система помехо- и имитоустойчивой передачи шифрованной информации в многоканальных системах однонаправленной радиосвязи на основе математического аппарата полиномиальных классов вычетов (модулярной арифметики). Особенностью системы является обеспечение ее новым свойством – восстановлением достоверной информации в условиях преднамеренных искажений (имитации) информации − имитоустойчивости.

Ключевые слова: *Имитозащита, имитоустойчивость, Китайская теорема об остатках, криптография, модулярная арифметика, полиномиальные классы вычетов, помехоустойчивое кодирование в классах вычетов, помехоустойчивые шифры, система остаточных классов.*

IMITATION PROOF DATA TRANSMITION IN PROTECTED SYSTEMS OF ONE-WAY COMMUNICATION BY MEANS OF POLYNOMIAL RESIDUE CLASSES

D.V. Samoylenko, O.A. Finko

The system described ensures the noise- and imitation proof of encrypted data in multi-channel systems of one-way radio communication by mathematically based means of polynomial residue classes (modular arithmetic). The singularity of the

system is its new feature – the recovery of authentic data in case of intended distortion (imitation) of data – imitation proof.

Key words: *Integrity protection, imitation stable, Chinese remainder theorem, cryptography, modular arithmetic, polynomial residue classes, error control codes in residue classes, interference stable ciphers, residue number system.*

Введение

Системы радиосвязи вообще и системы однонаправленной радиосвязи (системы оповещения, навигации, дистанционного управления и др.) в особенности, как известно, подвержены преднамеренным воздействиям и случайным помехам [1−3]. Если при этом используются, свойственные таким системам, криптографические методы защиты информации, то в связи с их высокой чувствительностью к ошибкам, возникающим при передаче информации, вопрос обеспечения помехоустойчивости и имитостойкости передаваемой информации приобретает выраженный проблемный характер [4, 5].

К недостаткам многих современных шифров следует отнести в целом не решенную проблему комплексного сбалансированного обеспечения классических требований: криптографической стойкости, имитостойкости и помехоустойчивости [4, с. 380]. Существующие методы противодействия имитации злоумышленника, такие как: формирование имитовставки или хэш кода, использование режимов шифрования, таких как гаммирование с обратной связью (ГОСТ 28149-89) в полной мере не решают этой задачи, так как не позволяют *восстанавливать* искаженные данные. Отсутствие решающей обратной связи в радионаправлениях существенно обостряет эту проблему.

В ряде работ [4−10] была предпринята попытка создания так называемых «помехоустойчивых шифров». Однако недостатком этих работ является либо частичность решения проблемы (борьба с отдельными видами ошибок типа «вставка», «выпадение» или «стирание» символов криптограммы и др.)

либо недостаточная изученность этих шифров, пока не допускающая возможность их практического применения.

В настоящей статье, являющейся продолжением работ [11−14], предлагается решение этой важной проблемы на основе использования существующих сертифицированных (и перспективных) блочных шифров, которое допускает возможность немедленного практического применения.

Имитоустойчивая передача шифрованной информации на основе избыточного модулярного полиномиального кода

В настоящее время в радионаправлениях для обеспечения требуемой криптографической стойкости и имитостойкости информации применяются шифры, а для обеспечения помехоустойчивости − методы помехоустойчивого кодирования [4, 6, 7, 10, 15]. При объединении в единую совокупность данных методов возможно получить новое качество системы передачи информации в радионаправлениях – *имитоустойчивость*, под которой здесь будем понимать способность системы к *восстановлению* достоверных шифрованных данных в условиях имитирующих действий злоумышленника, а также непреднамеренных помех.

В [11−14] была предложена система помехоустойчивой передачи конфиденциальной информации, основанная на свойствах избыточного модулярного кода, в которой сгенерированное в двоичном виде отправителем исходное сообщение M подлежит зашифрованию и разбивается на блоки фиксированной длины $M = \{M_1 | M_2 | \ldots | M_k\}$, здесь $|$ − символ конкатенации. i −й блок сообщения M_i представляется в полиномиальной форме:

$$M_i(z) = \sum_{i=0}^{s-1} m_j^{(i)} z^j = m_{s-1}^{(i)} z^{s-1} + m_{s-2}^{(i)} z^{s-2} + \ldots + m_0^{(i)},$$

$m_j^{(i)} \in \{0,1\}\ (i = 1, 2, \ldots, k;\ j = s-1, s-2, \ldots, 0)$.

Соответственно для получения последовательности блоков шифртекста $C_1(z), C_2(z), \ldots, C_k(z)$ потребуется выполнение k операций зашифрования, а для получения блоков $M_1(z)$, $M_2(z)$, $\ldots, M_k(z)$ открытого текста – k операций расшифрования. Процедуры зашифрования и расшифрования представляются в виде:

$$\begin{cases} C_1(z) \to E_{k_{e,1}} : M_1(z), \\ C_2(z) \to E_{k_{e,2}} : M_2(z), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ C_k(z) \to E_{k_{e,k}} : M_k(z), \end{cases}$$

$$\begin{cases} M_1(z) \to D_{k_{d,1}} : C_1(z), \\ M_2(z) \to D_{k_{d,2}} : C_2(z), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ M_k(z) \to D_{k_{d,k}} : C_k(z), \end{cases}$$

где $C_i(z)$ – блок шифртекста, $M_i(z)$ – блок открытого текста, $k_{e,1}, k_{d,1}$ – ключи (общий случай) зашифрования и расшифрования $(i = 1, 2, \ldots, k)$; соответственно при $k_{e,1} = k_{d,1}$ систему шифрования называют симметричной, а при $k_{e,1} \neq k_{d,1}$ – ассиметричной).

Принимаемые блоки шифртекста и, соответственно, блоки открытых текста обозначим как $C_1^*(z)$, $C_2^*(z)$, $\ldots, C_k^*(z)$ и $M_1^*(z)$, $M_2^*(z)$, $\ldots, M_k^*(z)$, так как они могут содержать искажения. Представим блоки шифртекста $C_i(z)$ как наименьшие неотрицательные вычеты по основаниям $m_i(z)$, таким что $\gcd(m_i(z), m_j(z)) = 1$, где $i \neq j$; $i, j = 1, 2, \ldots, k$. Причем $\deg C_i(z) < \deg m_i(z)$, где $\deg C_i(z)$ – степень полинома $(i = 1, 2, \ldots, k)$. Совокупность блоков шифртекста $C_1(z), C_2(z), \ldots, C_k(z)$ представим как единый суперблок шифртекста модулярного полиномиального кода (МПК) по системе оснований $m_1(z), m_2(z), \ldots, m_k(z)$. В соответствии с Китайской теоремой об остатках для многочленов [16, 17] для заданного множества многочленов $m_1(z), m_2(z), \ldots, m_k(z)$, удовлетворяющих условию $\gcd(m_i(z), m_j(z)) = 1$ и

многочленов $C_1(z), C_2(z),\ldots,C_k(z)$ таких, что $\deg C_i(z) < \deg m_i(z)$, система сравнений

$$\begin{cases} X(z) \equiv C_1(z) \mod m_1(z), \\ X(z) \equiv C_2(z) \mod m_2(z), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X(z) \equiv C_k(z) \mod m_k(z) \end{cases} \quad (1)$$

имеет единственное решение $X(z)$.

Выполним операцию расширения МПК $\{C_1(z), C_2(z),\ldots,C_k(z)\}_{\text{МПК}}$ путем введения r избыточных оснований $m_{k+1}(z), m_{k+2}(z),\ldots, m_{k+r}(z)$ и получения избыточных вычетов $C_{k+1}(z), C_{k+2}(z),\ldots,C_{k+r}(z)$:

$$\begin{cases} C_{k+1}(z) \equiv X(z) \mod m_{k+1}(z), \\ C_{k+2}(z) \equiv X(z) \mod m_{k+2}(z), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ C_{k+r}(z) \equiv X(z) \mod m_{k+r}(z). \end{cases}$$

Причем $\gcd(m_i(z), m_j(z)) = 1$, где $i \neq j$; $i, j = 1, 2,\ldots,k+r$ и $\deg m_1(z),\ldots, \deg m_k(z) < \deg m_{k+1}(z) < \ldots < \deg m_{k+r}(z)$. Получим расширенный МПК: $\{C_1(z), C_2(z),\ldots,C_k(z), C_{k+1}(z), C_{k+2}(z),\ldots, C_{k+r}(z)\}_{\text{МПК}}$ в кольце многочленов.

Структурная схема подсистемы имитоустойчивой передачи шифрованной информации представлена на рисунке 1, структура формируемых данных в подсистеме − на рисунке 2. Под одиночной ошибкой в кодовом слове МПК будем понимать произвольное искажение одного из блоков шифртекста кодового слова МПК, соответственно q-кратная ошибка определяется как произвольное искажение q блоков. Известно, что МПК обнаруживает q ошибок, при $r \geq q$, и исправляет q или менее ошибок, если $2q \leq r$ [18, 19].

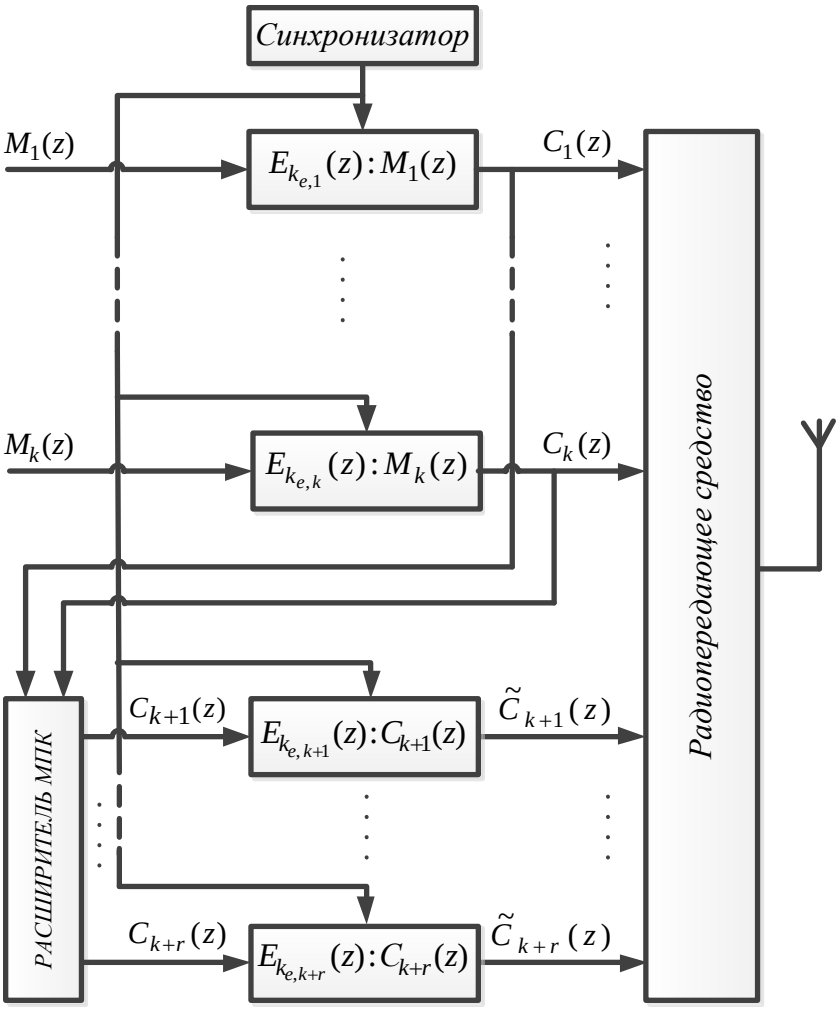


Рис. 1 Подсистема имитоустойчивой передачи шифрованной информации на основе МПК

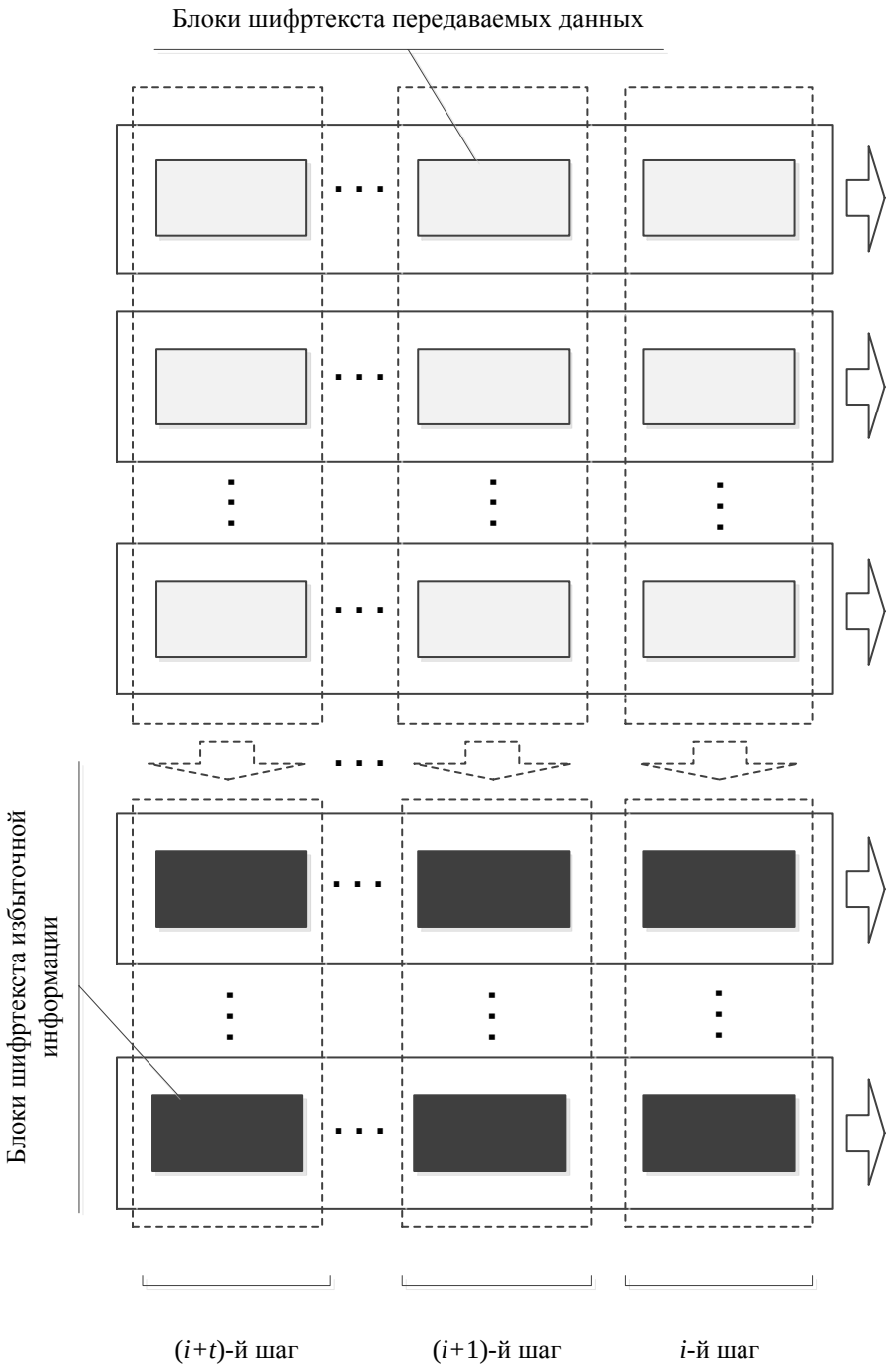


Рис. 2 Структура формируемых данных в подсистеме имитоустойчивой передачи шифрованной информации на основе МПК

В соответствии с правилами декодирования модулярных кодов критерием отсутствия обнаруживаемых ошибок в модулярном коде [18–25] и МПК в частности $\{C_1^*(z),\ldots,C_k^*(z),\ldots,C_{k+r}^*(z)\}_{\text{МПК}}$, является выполнение неравен-

ства: $\deg X^*(z) < \deg P_k(z)$, где $P_k(z) = \prod_{i=1}^{k} m_i(z)$ и $X^*(z)$ – решение системы сравнений (1) для $C_1^*(z), \ldots, C_k^*(z), \ldots, C_{k+r}^*(z)$. Критерий существования обнаруживаемой ошибки – выполнение неравенства: $\deg X^*(z) \geq \deg P_k(z)$, где символ * указывает на наличие возможных искажений в кодовом слове [24, 25]. Структурная схема подсистемы имитоустойчивого приема шифрованной информации представлена на рисунке 3.

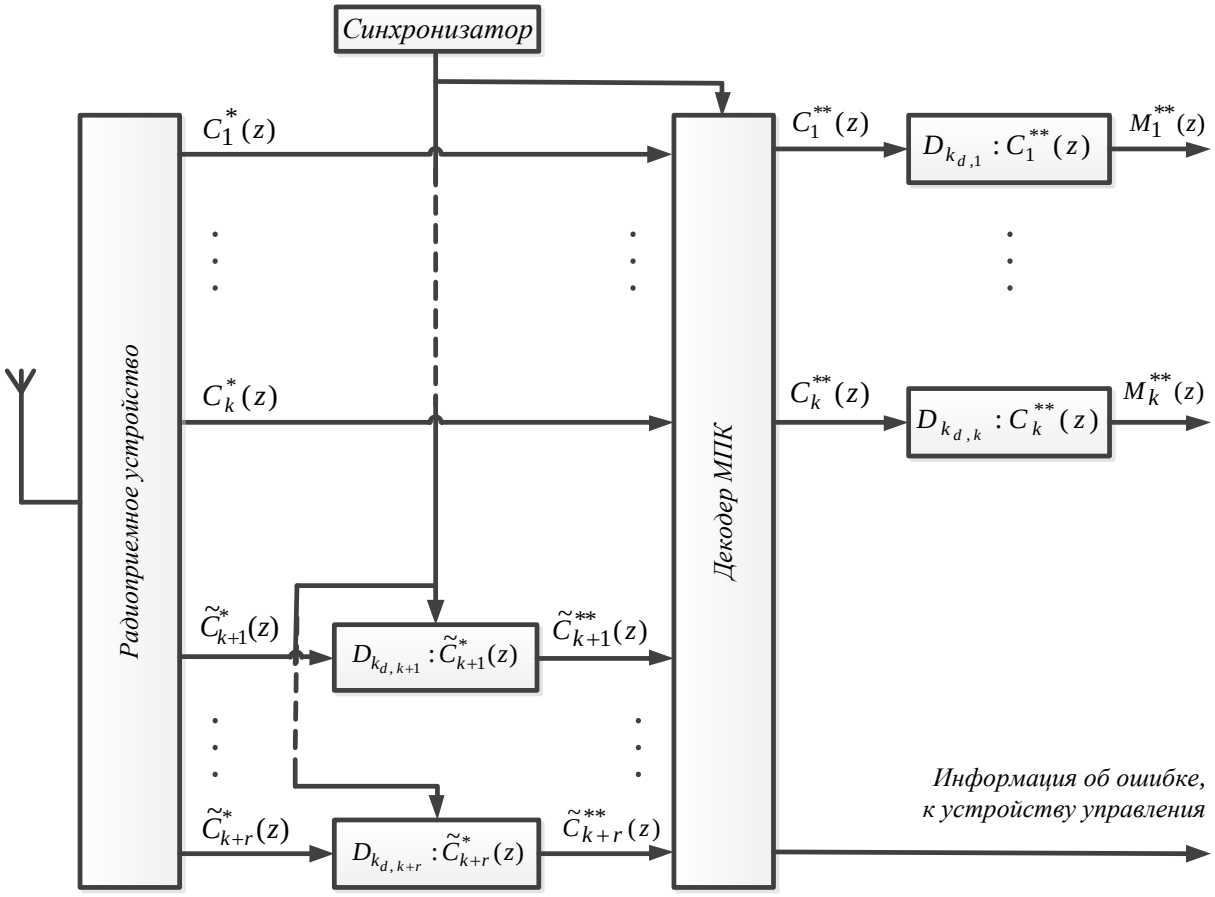


Рис. 3 Подсистема имитоустойчивого приема шифрованной информации на основе МПК

Использование имитовставок

Особенностью представленной выше системы является необходимость введения избыточной шифрованной информации в соответствии со свой-

ствами МПК и заданными требованиями к кратности обнаруживаемых или исправляемых искажений в передаваемых данных. В настоящее время для обнаружения имитации злоумышленника в канале связи применяется дополнительный режим шифрования ГОСТ 28147-89 – режим выработки имитовставки. Недостатком данного способа противодействия имитации является отсутствие возможности восстановления достоверной информации в однонаправленных (без обратной связи) системах передачи информации. Комплексирование метода обеспечения имитозащищенности данных на основе выработки имитовставок и представленного выше решения, основанного на расширении МПК с шифрованием избыточной информации, должно позволить преодолеть недостаток известного решения.

Пусть имитовставки образуются как обычно из последовательности, состоящей из l блоков шифртекста. Представим процедуру выработки имитовставок $H_i(z)$ $(i=1, 2, \ldots, k)$ в виде:

$$\begin{cases} H_1(z) \to I_{h_1} : \mathbf{C}_1(z), \\ H_2(z) \to I_{h_2} : \mathbf{C}_2(z), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ H_k(z) \to I_{h_k} : \mathbf{C}_k(z), \end{cases}$$

где $\mathbf{C}_i(z)=[C_{i,1}(z) \quad C_{i,2}(z) \quad \ldots \quad C_{i,l}(z)]$ – векторное представление суперблока шифртекста, I_{h_i} – оператор выработки имитовставки на ключе h_i $(i=1, 2, \ldots, k)$, l – длина суперблока. Целенаправленное воздействие злоумышленника на процесс передачи суперблоков шифртекста с вычисленными от них имитовставками влечет за собой их возможное искажение. Соответственно на приемной стороне от суперблоков $\mathbf{C}_i^*(z)=[C_{i,1}^*(z) \quad C_{i,2}^*(z) \quad \ldots \quad C_{i,l}^*(z)]$ $(i=1, 2, \ldots, k)$ шифртекста вычисляются имитовставки:

$$\begin{cases} \tilde{H}_1(z) \to I_{h_1} : \mathbf{C}_1^*(z), \\ \tilde{H}_2(z) \to I_{h_2} : \mathbf{C}_2^*(z), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \tilde{H}_k(z) \to I_{h_k} : \mathbf{C}_k^*(z). \end{cases}$$

Так же как и в предыдущем решении для восстановления имитируемых злоумышленником сообщений из передаваемой последовательности суперблоков шифртекста с имитовставками $\{\mathbf{C}_1(z), H_1(z)\};\{\mathbf{C}_2(z), H_2(z)\};\ldots;\{\mathbf{C}_k(z), H_k(z)\}_{\text{МПК}}$ строится расширенный МПК. Структурная схема подсистемы отправителя с одним избыточным каналом шифрования представлена на рисунке 4, структура формируемых данных при этом представлена на рисунке 5.

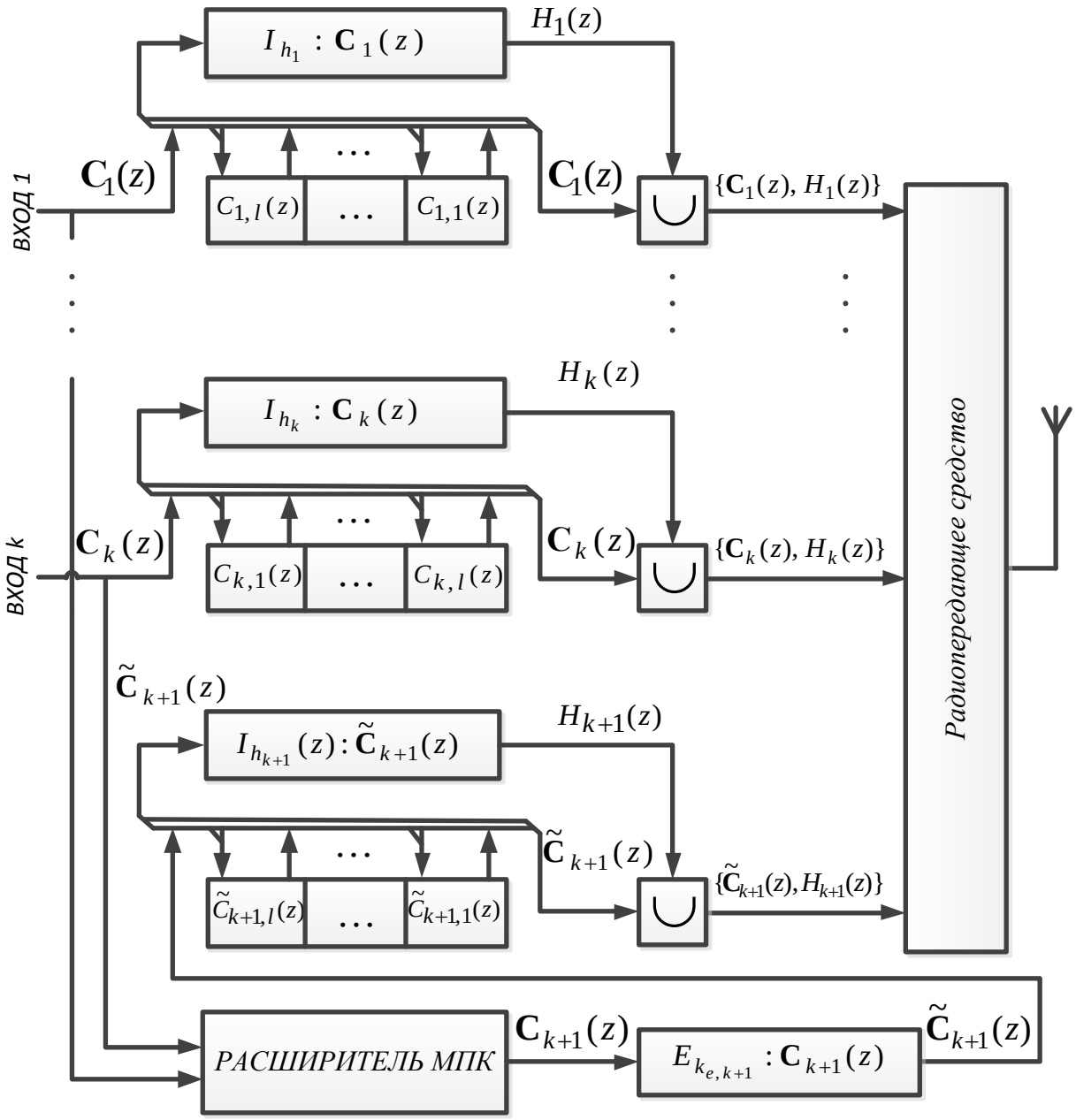


Рис. 4 Подсистема имитоустойчивой передачи шифрованной информации на основе МПК и использования имитовставок (частный случай – с одним избыточным каналом)

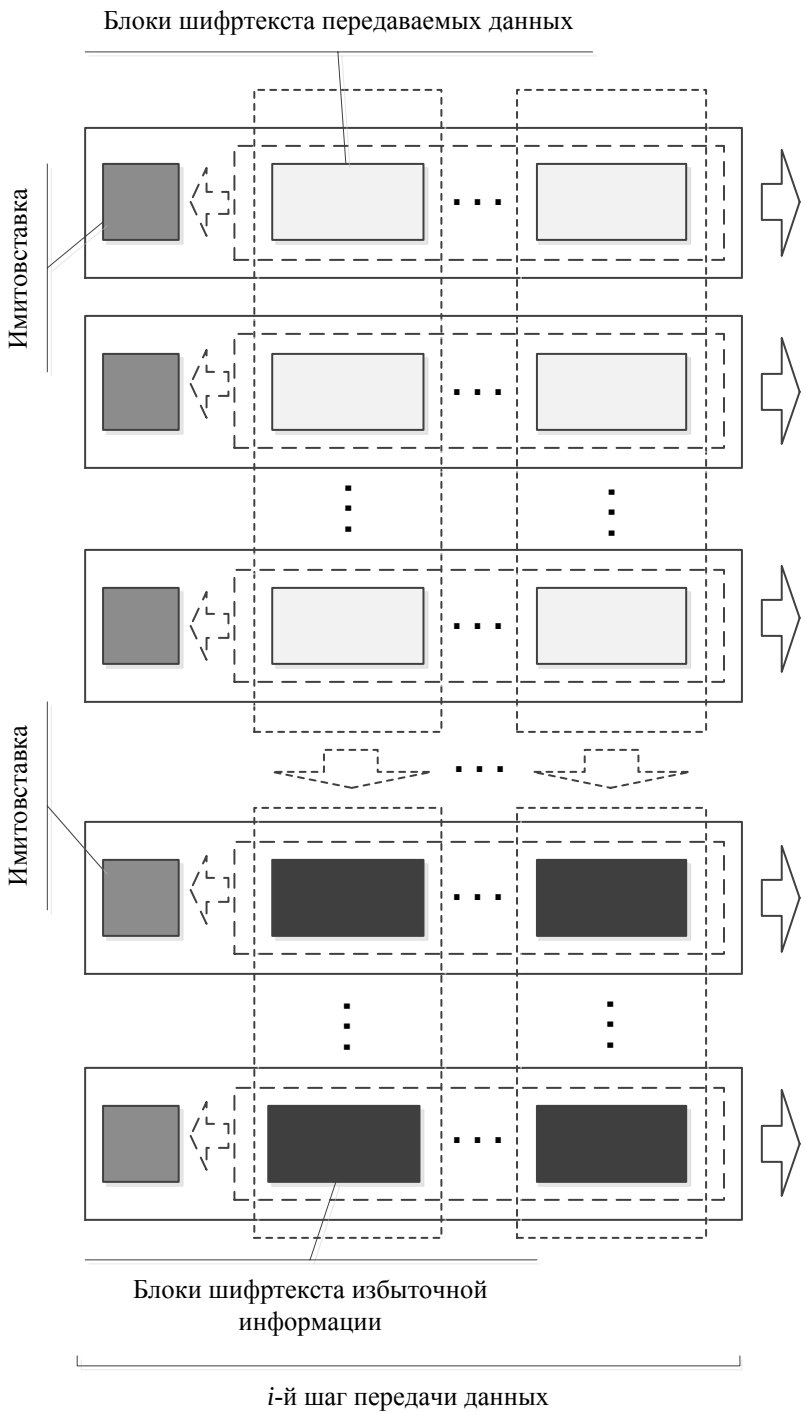


Рис. 5 Структура формируемых данных в подсистеме имитоустойчивой передачи шифрованной информации на основе МПК и использования имитовставок

Подсистема имитоустойчивого приема шифрованной информации на основе МПК и использования имитовставок представлена на рисунке 6 и реализует следующий алгоритм.

Вход: принятая последовательность суперблоков шифрекста с имитовставками: $\{\mathbf{C}_1^*(z), H_1^*(z)\};\ldots;\{\mathbf{C}_k^*(z), H_k^*(z)\};\{\tilde{\mathbf{C}}_{k+1}^*(z), H_{k+1}^*(z)\}$.

Выход: исправленная (восстановленная) совокупность суперблоков шифртекста $\mathbf{C}_1^{**}(z),\ldots,\mathbf{C}_k^{**}(z)$ (** − указывают на вероятностный характер восстановления).

Шаг 1. Обнаружение возможной имитации злоумышленника в принятой последовательности суперблоков шифртекста с локализацией номера i канала с выявленными ложными блоками шифртекста путем сравнения имитовставок, полученных из канала связи $H_1^*(z),\ldots,H_k^*(z),H_{k+1}^*(z)$ и имитовставок $\tilde{H}_1(z),\ldots,\tilde{H}_k(z),\tilde{H}_{k+1}(z)$, вычисленных в подсистеме приема данных. На выходах блоков сравнений (БС) для всех $i=1,2,\ldots,k,k+1$ формируются сигналы:

$$\begin{cases}1, & \text{если} \quad H_i^*(z)\neq\tilde{H}_i(z);\\ 0, & \text{если} \quad H_i^*(z)=\tilde{H}_i(z).\end{cases}\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Шаг 2. Восстановление достоверных данных путем решения систем сравнений:

$$\begin{cases}
\begin{cases}
X_1^{**}(z) \equiv C_{J_1,1}^{*}(z) \mod m_{J_1}(z), \\
X_1^{**}(z) \equiv C_{J_2,1}^{*}(z) \mod m_{J_2}(z), \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_1^{**}(z) \equiv C_{J_k,1}^{*}(z) \mod m_{J_k}(z);
\end{cases} \\
\begin{cases}
X_2^{**}(z) \equiv C_{J_1,2}^{*}(z) \mod m_{J_1}(z), \\
X_2^{**}(z) \equiv C_{J_2,2}^{*}(z) \mod m_{J_2}(z), \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_2^{**}(z) \equiv C_{J_k,2}^{*}(z) \mod m_{J_k}(z);
\end{cases} \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\begin{cases}
X_l^{**}(z) \equiv C_{J_1,l}^{*}(z) \mod m_{J_1}(z), \\
X_l^{**}(z) \equiv C_{J_2,l}^{*}(z) \mod m_{J_2}(z), \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_l^{**}(z) \equiv C_{J_k,l}^{*}(z) \mod m_{J_k}(z).
\end{cases}
\end{cases} \qquad (2)$$

или

$$\begin{cases}
\mathbf{X}^{**}(z) \equiv \mathbf{C}_{J_1}^{*}(z) \mod m_{J_1}(z), \\
\mathbf{X}^{**}(z) \equiv \mathbf{C}_{J_2}^{*}(z) \mod m_{J_2}(z), \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\mathbf{X}^{**}(z) \equiv \mathbf{C}_{J_k}^{*}(z) \mod m_{J_k}(z).
\end{cases}$$

где $J_1, J_2, \ldots, J_k$ – номера каналов, результат сравнения имитовставок для которых показал отсутствие искажений в j-м суперблоке шифртекста $\mathbf{C}_j^{*} = [C_{j,1}^{*}(z) \quad C_{j,2}^{*}(z) \quad \ldots \quad C_{j,l}^{*}(z)]$.

В соответствии с Китайской теоремой об остатках для многочленов решениями систем (2) являются:

$$X_j^{**} = C_{J_1,j}^{*}(z)B_{j_1}(z) + C_{J_2,j}^{*}(z)B_{J_2}(z) + \ldots + C_{J_k,j}^{*}(z)B_{J_k}(z) \bmod P_{k_\nu}(z),$$

где $B_{J_i}(z) = k_{J_i}(z)P_i(z)$ – полиномиальные ортогональные базисы, $P_{k_\nu}(z) = \prod\limits_{\substack{i=1\ldots k; \\ i\neq\nu}} m_i$, ν – номер выявленного «недостоверного» канала,

$$P_{J_i}(z)=\frac{P_{k_v}(z)}{m_i(z)}, \quad k_{J_i}(z)=P_{J_i}^{-1}(z) \bmod m_{J_i}(z) \qquad (i=1, 2, \ldots, k;\ J_i=1, 2, \ldots, k+1).$$

Значения полиномиальных ортогональных базисов рассчитываются заблаговременно и хранятся в памяти декодера МПК [26].

Восстановление достоверных блоков может быть выполнено путем вычисления наименьших вычетов:

$$\begin{cases} C_{1,\,j}^{**}(z)=X_j^{**}(z) \mod m_1, \\ C_{2,\,j}^{**}(z)=X_j^{**}(z) \mod m_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ C_{k,\,j}^{**}(z)=X_j^{**}(z) \mod m_k, \end{cases}$$

или любым другим известным методом декодирования избыточных МПК.

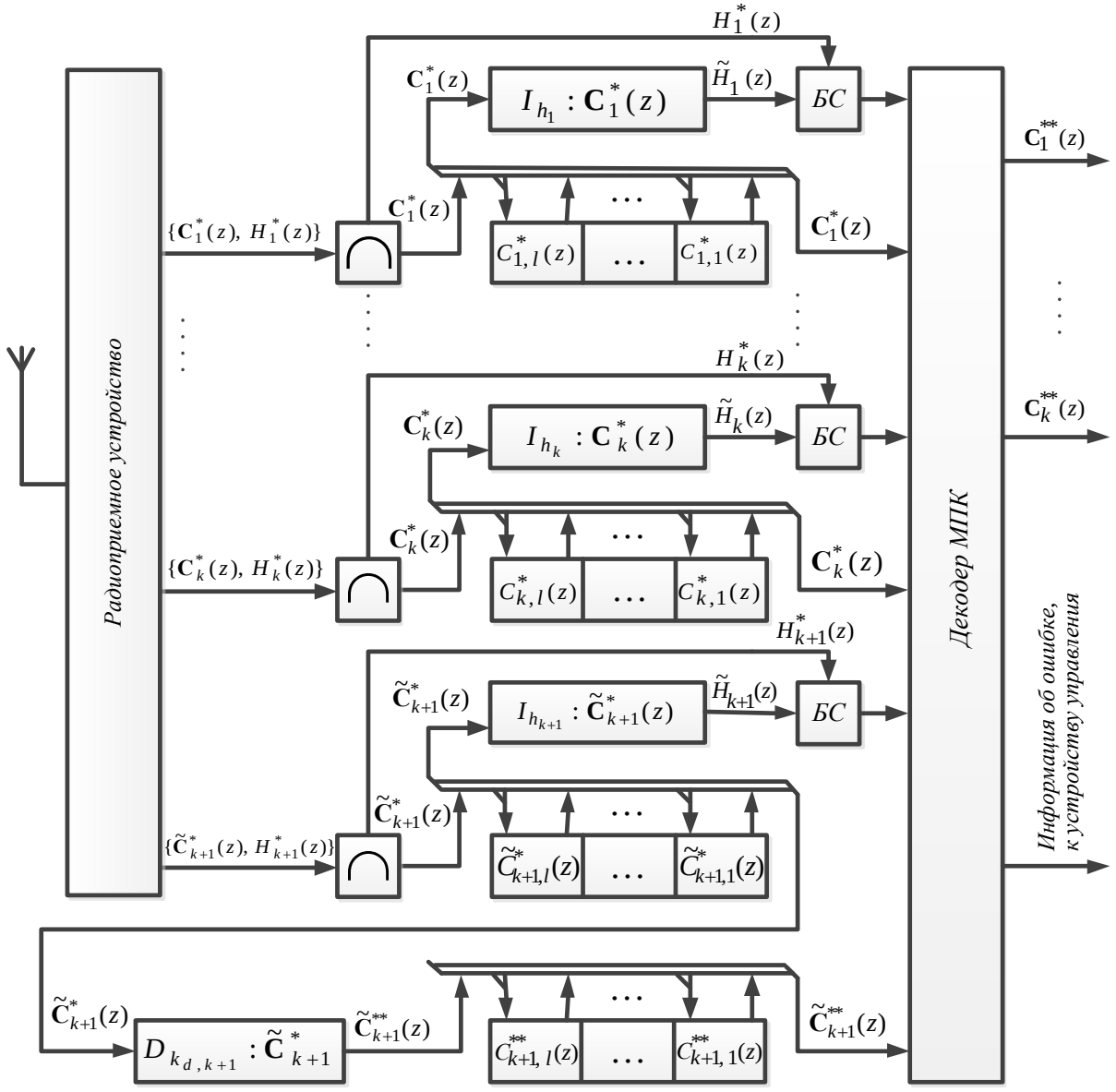
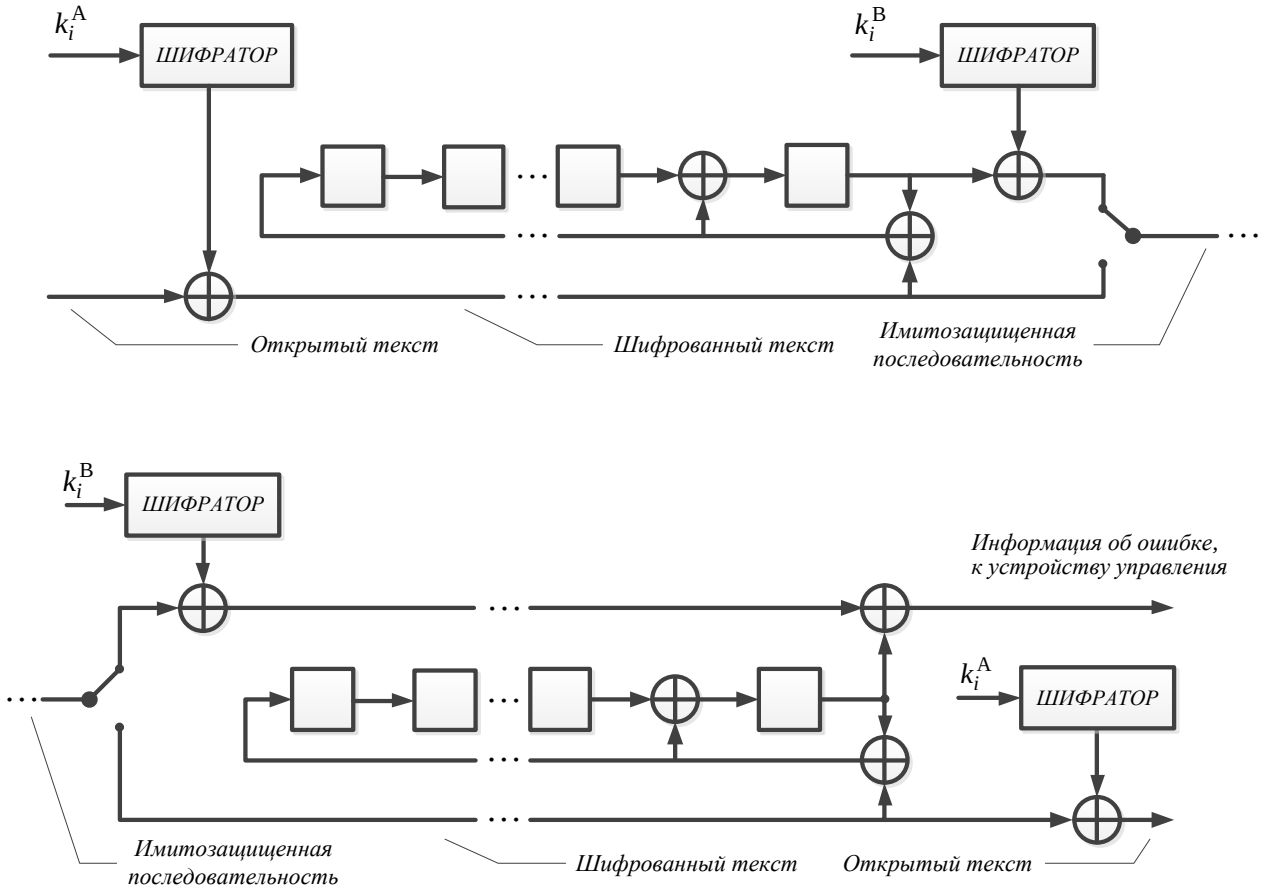


Рис. 6 Подсистема имитоустойчивого приема шифрованной информации на основе МПК и использования имитовставок (частный случай с одним избыточным каналом)

Имитозащищенная поточная передача шифрованной информации

Рассмотренный метод построения имитоустойчивых систем для блочных шифров может быть обобщен и для поточных систем передачи шифро-

ванной информации. В качестве примера с помощью рисунка 7 поясняется принцип формирования и декодирования имитозащищенных последовательностей на основе разделимого сверточного кода [1]. Криптосистемы, используемые в шифраторах для решения задач крипто- (на ключах k_i^{A}) и имитозащиты (на ключах k_i^{B}), в принципе, могут отличаться друг от друга, так как имеют различные назначения. Информация об ошибках на выходе приемного устройства (рис. 7б) может трактоваться как результат воздействия помех в канале связи, так и как результат преднамеренных действий злоумышленника, которому известны алгоритмы формирования сверточных кодов. Злоумышленник не может вычислить и подменить избыточные символы, соответствующие новому (имитируемому) шифртексту, так как для этого ему необходимо вскрыть систему шифрования (на ключах k_i^{B}), используемую для обеспечения имитозащищенности. При этом отличить результат действия помех от действий злоумышленника в принципе возможно, используя статистический метод анализа сигналов об обнаруженных ошибках. Возможен вариант применения вторичного поточного кодирования передаваемых данных, предназначенного для обеспечения заданной помехоустойчивости в канале связи. Сигналы об ошибках, выдаваемые схемой (рис. 7б), в сочетании с анализом информации выдаваемой вторичным декодером (злоумышленник знает алгоритм формирования вторичного кода) могут указывать на возможные имитирующие действия злоумышленника.



а)

б)

Рис. 7 Пояснение принципа построения системы имитозащищенной передачи сообщений, основанной на разделимых сверточных кодах: а) кодер, б) декодер

Выводы

Предложенный метод обеспечения имитоустойчивости передачи шифрованных данных обеспечивает обнаружение имитирующих действий злоумышленника в канале радиосвязи и, при необходимости, восстановление достоверных данных с заданной вероятностью. Последнее качество полезно для систем передачи информации, не имеющих обратной связи, в условиях ограничений на время передачи данных. Использование имитовставок, с од-

ной стороны, позволяет уменьшить избыточность МПК и обеспечить возможность исправления ошибок кратности, соответствующей его обнаруживающим способностям. С другой стороны, использование имитовставок вносит дополнительную избыточность в передаваемые данные, однако необходимость использования имитовставок может быть обусловлена требованиями заказчика и требованиями уровню обеспечиваемой имитозащиты.

С точки зрения криптоанализа использование в целях обеспечения имитоустойчивости исключительно МПК (без имитовставок) представляет собой относительно упрощенную задачу для криптоаналитика, основанную на атаке «при известном открытом тексте». Однако «открытый текст» здесь – передаваемые зашифрованные данные, что не влечет за собой снижения криптостойкости этих данных. Для повышения имитостойкости представленные решения могут быть усовершенствованы путем введения процедур перешифрования защищенных данных (на новых ключах), исключающих возможность применения подобной атаки.

Не смотря на то, что представленные решения основываются на использовании методов помехоустойчивого кодирования данных, следует заметить, что они не исключают возможность и необходимость применения классических методов борьбы со случайными ошибками в канале связи, в том числе и методы помехоустойчивого кодирования в традиционном их понимании.

Литература

1. Финк Л.М. Теория передачи дискретных сообщений. М.: Советское радио, 1970. 728 с.

2. Кловский Д.Д. Передача дискретных сообщений по радиоканалам. М.: Радио и связь, 1982. 304 с.

3. Макаров С.Б., Цикин И.А. Передача дискретных сообщений по радиоканалам с ограниченной полосой пропускания. М.: Радио и связь, 1988. 304 с.

4. Бабаш А.В., Шанкин Г.П. Криптография. М.: Солон-Р, 2002. 512 с.

5. Диффи У., Хеллман М. Защищенность и имитостойкость. Введение в криптографию // ТИИЭР. 1979. т.64, №3. С. 71-109.

6. Бабаш А.В., Глухов М.М., Шанкин Г.П. О преобразованиях множества слов в конечном алфавите, не размножающие искажений // Дискретная математика. 1979. т.9, №3. С. 3-19.

7. Тилборг ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. М.: Мир, 2006. 471 с.

8. McEliece R.J. A Public‑Key Cryptosystem Based on Algebraic Coding Theory, Deep Space Network Progress Report 42‑44, Jet Propulsion Laboratory. California Institute of Technology. 1978. p. 114–116.

9. Niederreiter H. Knapsack–Type Cryptosystems and Algebraic Coding Theory // Problems of Control and Information Theory. 1986. 15(2). p. 159–166.

10. Godoy W. A proposal of a cryptography algorithm with techniques of error correction // Computer Communications. 1997. 20(15). P. 1374.

11. Финько О.А. Групповой контроль ассиметричных криптосистем методами модулярной арифметики // XIV Междунар. школа-семинар «Синтез и сложность управляющих систем»: сб. науч. тр. / под ред. акад. РАН О.Б. Лупанова. МГУ им. М.В. Ломоносова; Н. Новгород: Изд-во Нижегород. пед. ун-та, 2003. С. 85–86.

12. Финько О.А. Многоканальные системы, устойчивые к искажению криптограмм: в коллект. монограф. «Криптографические методы защиты информации» / под ред. Е.А. Сухарева. М.: Радиотехника, 2007. Кн. 4. С. 91–96.

13. Финько О.А., Самойленко Д.В. Конструкции, контролирующие ошибки, на основе действующих криптографических стандартов // VIII Меж-

дунар. конф. «Дискретные модели в теории управляющих систем»: сб. науч. тр. М.: Изд-во МГУ им. М.В. Ломоносова, 2009. С. 318–320.

14. Самойленко Д.В., Финько О.А. Криптографическая система в полиномиальных классах вычетов для каналов с шумом и имитирующим злоумышленником // Теория и техника радиосвязи. 2010. № 4. С. 39–45.

15. Основы криптографии : учеб. пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин [и др.]. М.: Гелиос АРВ, 2002. 480 с.

16. Габидулин Э.М., Афанасьев В.Б. Кодирование в радиоэлектронике. М.: Радио и связь, 1986. 176 с.

17. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986. 576 с.

18. Акушский И.Я., Юдицкий Д.М. Машинная арифметика в остаточных классах. М.: Советское радио, 1968. 440 с.

19. Бояринов И.М. Помехоустойчивое кодирование числовой информации. М.: Наука, 1983. 196 с.

20. Szabo N.S., Tanaka R.I. Residue Arithmetic and its Applications Computer Technolog. New York: McGraw-Hill, 1967. P. 236.

21. Амербаев В.М. Теоретические основы машинной арифметики. Алма-Ата: Наука, 1976. 324 с.

22. Торгашев В.А. Система остаточных классов и надежность ЦВМ. М.: Советское радио, 1973. 120 с.

23. Mandelbaum D.M. Error correction in residue arithmetic // IEEE Trans. Comput. 1972. 21(6). p. 538–545.

24. Калмыков И.А. Математические модели нейросетевых отказоустойчивых вычислительных средств, в полиномиальной системе классов вычетов / под ред. Н.И. Червякова. М.: ФИЗМАТЛИТ, 2005. С. 68–159

25. Mandelbaum D.M. A method of coding for multiple errors // IEEE Trans. On Information Theory. 1968. 14(3). p. 518–521.

26. Финько О.А. Контроль и реконфигурация аналого-цифровых устройств, функционирующих в системе остаточных классов // Электронное моделирование. 2000. т.22. №4. С. 92–103.

Самойленко Дмитрий Владимирович − (1983), канд. техн. наук., ст. преподаватель кафедры филиала Военной академии связи (г. Краснодар).
Область научных интересов: полиномиальные классы вычетов и их применение в защищённых системах связи. E-mail: 19sam@mail.ru

Финько Олег Анатольевич − (1963), докт. техн. наук, профессор кафедры филиала Военной академии связи (г. Краснодар).
Область научных интересов: модулярная арифметика, параллельные логические вычисления, криптографическая защита информации.
E-mail: ofinko@yandex.ru; URL: http://ofinko.ru/

Samojlenko Dmitry − (1983), PhD. tehn. Science., Art. Lecturer branch of the Military Academy of Communications (Krasnodar).
Research interests: the polynomial residue classes and their application in secure communication systems. E-mail: 19sam@mail.ru

Finko Oleg − (1963), Doctor. tehn. Sciences, Department of the branch of the Military Academy of Communications (Krasnodar).
Research interests: modular arithmetic, logical parallel computing, cryptographic protection of information.
E-mail: ofinko@yandex.ru; URL: http://ofinko.ru/