# В.А. ЛИТВИНОВ, С.Я. МАЙСТРЕНКО, Ю.Г. ПИЛИПЕНКО

# ИСПРАВЛЕНИЕ ОШИБОК ПОЛЬЗОВАТЕЛЯ НА ОСНОВЕ СОВМЕСТНОГО ПРИМЕНЕНИЯ ПОМЕХОЗАЩИТНЫХ КОДОВ И ВИРТУАЛЬНОГО СЛОВАРЯ ДОПУСТИМЫХ СЛОВ

**Abstract:** The descibed model of the automatic error correction is based on the joint application of the code methods and method of the inverse distortion for increasing validity of the input information and saving labor of error correction. The combined algorithms of automatic and semiautomatic error correction are considered. For the proposed algorithms, probabilistic estimations of the automatic, semiautomatic, manual and false correction, which can be used while deciding which algorithm of adjustment to choose, are analytically derived.

Key words: user errors, automatic correction, data reliability, error-correcting coding.

**Анотація:** Описана модель автоматичного виправлення помилок ґрунтується на сумісному використанні кодових методів та методу зворотних спотворень для підвищення достовірності вхідної інформації й зниження трудомісткості виправлення помилок. Розглядаються комбіновані алгоритми автоматичної та напівавтоматичної корекції помилок. Для запропонованих алгоритмів аналітично отримані ймовірнісні оцінки автоматичної, напівавтоматичної, ручної та хибної корекції, які можуть використовуватись при прийнятті рішень відносно вибору алгоритму корекції.

Ключові слова: помилки користувача, автоматична корекція, достовірність даних, перешкодозахисні коди.

**Аннотация:** Описанная модель автоматического исправления ошибок основана на совместном применении кодовых методов и метода обратных искажений для повышения достоверности входной информации и снижения трудоемкости исправления ошибок. Рассматриваются комбинированные алгоритмы автоматической и полуавтоматической коррекции ошибок. Для предлагаемых алгоритмов аналитически получены вероятностные оценки автоматической, полуавтоматической, ручной и ложной коррекции, которые могут быть использованы при принятии решений относительно выбора алгоритма корректировки.

**Ключевые слова:** ошибки пользователя, автоматическая коррекция, достоверность данных, помехозащитные коды.

# 1. Введение

Известны и описаны в литературе методы помехозащитного кодирования, предназначенные для повышения достоверности входной алфавитно-цифровой информации путем автоматического исправления ошибок пользователя. Наиболее полный обзор таких методов приведен в [1]. Большинство этих методов ориентировано на автоматическое исправление однократных ошибок типа замены значения одного символа и обнаружение с последующим «ручным» исправлением ошибок иных классов.

Помехозащитные коды с исправлением ошибок (КИО) применяются для защиты информации в каналах связи, где вероятность появления ошибок, кратности более 1, значительно, на несколько порядков меньше вероятности однократной ошибки. Поэтому относительное количество не автоматически исправленных ошибок сравнительно невелико. Для информации, вводимой пользователем, положение иное. Здесь, как известно, ошибки типа, например, пропуска символа имеют кратность от 1 до n в зависимости от позиции пропущенного символа, а вероятность такой ошибки не намного меньше вероятности однократной транскрипции. По этим причинам относительное количество вручную исправляемых ошибок здесь может быть значительным.

Метод, позволяющий в этих случаях уменьшить долю ошибок, исправляемых вручную, и снизить тем самым общую трудоемкость ввода и корректировки информации, заключается в расширении штатной процедуры декодирования КИО за счет привлечения метода обратных искажений («вариаций» ошибочного слова) и проверки корректности значения вариации по

словарю допустимых слов [2]. При отсутствии реального словаря в качестве такового может быть использован *виртуальный* словарь (см. далее).

В статье решается задача построения модели и оценки существенных характеристик метода.

# 2. Постановка задачи и алгоритм декодирования и исправления ошибок

Введем следующие обозначения и допущения:

 $q, n_u, n_k$  — соответственно алфавит, количество информационных символов, количество контрольных символов входного слова,  $n_u + n_k = n$  ;

 $\mathbf{E} = \left\{ E_i \right\}$  – множество классов возможных ошибок;

 $p_i$  – относительное количество ошибок класса  $E_i$  в потоке вводимых слов;

 ${f E}_k^1$  — подмножество классов ошибок, на автоматическое исправление которых ориентирован конкретный КИО, и назовем их первично корректируемыми ошибками;

 ${f E}_k^2$  – подмножество классов ошибок, идентифицируемых виртуальным словарем (вторично корректируемые ошибки);

T – виртуальный словарь – множество слов, удовлетворяющих условию отсутствия ошибки, определенному контрольным соотношением (алгоритмом кодирования-декодирования) используемого КИО. Мощность T не превышает  $q^n$ ;

 $r = \frac{1}{q^{n_k}}$  - коэффициент избыточности кода, определяющий относительное количество

всевозможных комбинаций значений n символов, не удовлетворяющих условию вхождения в T .

Примем допущение, что значения вариаций ошибочного слова случайно распределены среди  $q^n$  всевозможных значений слов. В этом случае процесс генерации вариаций и их сравнения с T мы можем описать моделью испытаний Бернулли, для которой вероятность P(g,r,V) случайного совпадения в точности g вариаций из V проверяемых, при условии, что вероятность одного случайного совпадения равна r определяется известной формулой биноминального распределения:

$$P(g,r,V) = C_V^g r^g V^{V-g}.$$

Общая схема комбинированной процедуры включает два этапа.

- 1. Декодирование слова (кода) стандартной процедурой, присущей используемому КИО.
  - 1.1. Идентификация слова как правильного или ошибочного.
- 1.2. Если в слове имеется ошибка, принадлежащая множеству  $\mathbf{E}_k^1$ , то она обнаруживается и автоматически исправляется. Иначе, слово идентифицируется как неисправимо ошибочное (в смысле возможностей кода). Переход к этапу 2.

2. Генерация V вариаций в классах ошибок, принадлежащих множеству  $\mathbf{E}_k^2$ , и проверка каждой вариации слова на принадлежность T (т.е., по сути, многократное повторение этапа 1 для генерируемых вариаций). В зависимости от результатов проверки возможно автоматическое или полуавтоматическое исправление в соответствии с алгоритмами, описанными в [2].

При этом возможны следующие финальные исходы.

 $R_{AK}$ ,  $R_{IIAK}$  — ошибка правильно идентифицирована и исправлена автоматически (вероятность  $P_{AK}$ ) или полуавтоматически, т.е. с подтверждением пользователя (вероятность  $P_{IIAK}$ );

 $R_{P\!K}$  – идентифицировать ошибку не удается и она исправляется полностью "вручную" (вероятность  $P_{P\!K}$ );

 $R_{\it ЛK}$  – ошибка идентифицирована неверно и исправлена ложно (вероятность  $P_{\it ЛK}$  ).

Определение этих вероятностей и является целью построения следующих моделей. Под вероятностями здесь и далее понимается относительное количество исходов, "благоприятных" в определенном конкретном смысле.

#### 3. Общая модель

3.1. Вероятностные характеристики метода (значения  $P_{AK}$ ,  $P_{PK}$ ,  $P_{DK}$ ) для автоматической вторичной корректировки (алгоритм A) определяет вероятностно-логический граф, приведенный на рис. 1. За основу принят алгоритм однозначной корректировки вторично корректируемой ошибки [2]. В этом случае автоматическое исправление ошибок  $\mathbf{E}_k^2$  производится только при единственном совпадении вариации со словарем (т.е. при отсутствии синонимов).

Последовательность x дуг графа означает совместное наступление x независимых событий; финальная вероятность последнего события равна произведению вероятностей, приписанных каждой дуге; разветвление y дуг означает наступление одного из y несовместных событий; суммарная вероятность событий по y разветвляющимся дугам, равная сумме соответствующих вероятностей, должна быть равна 1, как полная группа событий. Сумма финальных вероятностей по листьям дерева должна быть равна 1, а для искомых вероятностей P должны выполняться условия:

$$P_{AK} + P_{PK} + P_{JJK} + P_{HO} = 1;$$

$$P_{AK}, P_{PK}, P_{JK}, P_{HO} \in [0,1].$$

Таким образом, приведенный граф отражает структуру финальных вероятностей независимых событий.

На рис. 1 приняты следующие обозначения событий и их вероятностей:

 $S_o$  – ошибка произошла;

 $S_1$  — ошибка  $\in \mathbf{E}^1_k$  , вероятность этого события  $\mathcal{\Pi}_1$  равна относительному количеству первично обнаруживаемых ошибок  $P_1$  ;

 $S_2 = \overline{S}_1$  – ошибка  $\not\in \ \mathbf{E}_k^1$  с вероятностью  $\mathbf{\pi}_2 = 1 - P_1$ ;

 $\mathbf{S}_{21}$  – ошибка обнаружена с вероятностью  $oldsymbol{\mathcal{\pi}}_{2l} = l - r$  ;

 $\mathbf{S}_{22}=\overline{\mathbf{S}}_{21}$  – ошибка не обнаружена с вероятностью  $oldsymbol{\mathcal{H}}_{22}=r$  ;

 ${f S}_{211}$  – ошибка принята для идентификации и исправления с вероятностью  ${m \mathcal{I}}_{211}=1-{m eta}$  ;

 $S_{212} = \overline{S}_{211}$  – ошибка ложно исправлена кодом с вероятностью  $m{\mathcal{I}}_{212} = m{eta}$  ;

 $\mathbf{S}_{2111}$  – ошибка  $\in \mathbf{E}_{k}^{2}$  с вероятностью  $oldsymbol{\pi}_{2111} = P_{2}$ ;

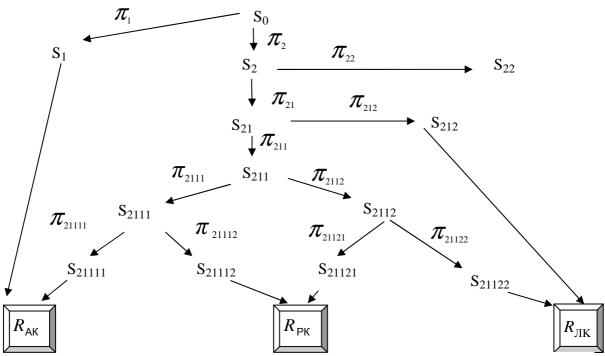


Рис. 1. Граф частных событий для алгоритма автоматического исправления

 $\mathbf{S}_{2112}=\overline{\mathbf{S}}_{2111}$  – ошибка  $otin\mathbf{E}_{k}^{2}$  с вероятностью  $otag{\mathbf{\pi}}_{2112}=\mathbf{1}-P_{2}$  ;

 $\mathbf{S}_{21111}$  – ошибка однозначна (z=1) с вероятностью  $\mathbf{\pi}_{21111} = P(0,r,V-1) = (1-r)^{V-1}$ ;

 ${
m S}_{{
m 21112}}=\overline{
m S}_{{
m 21111}}$  – ошибка многозначна ( z>1 ) с вероятностью

$$\boldsymbol{\pi}_{21112} = \sum_{g=1}^{V-1} P(g,r,V-1) = 1 - P(0,r,V-1);$$

 $S_{21121}$  — для ошибки, которая не принадлежит  ${f E}_k^2$ , не состоялось ни одного случайного совпадения вариаций со словом словаря (z=0) с вероятностью  ${f \pi}_{21121}=1-P(1,r,V)=1-rV(1-r)^V$ ;

 $\mathbf{S}_{21122}=\overline{\mathbf{S}}_{21121}$  — ошибка, которая не принадлежит  $\mathbf{E}_k^2$ , однозначна ( z=1 ) с вероятностью  $oldsymbol{\pi}_{21122}=\mathrm{P}(1,r,V_c)=rV(1-r)^V_c$  .

С учетом приведенных обозначений и вида графа рис. 1 можно записать такие логические выражения:

$$\begin{split} R_{AK} &= S_{1} \vee \left(S_{2} \wedge S_{2I} \wedge S_{2II} \wedge S_{2III} \wedge S_{211I1}\right); \\ R_{PK} &= \left(S_{2} \wedge S_{2I} \wedge S_{2II}\right) \wedge \left(\left(S_{2111} \wedge S_{21112}\right) \vee \left(S_{2112} \wedge S_{21121}\right)\right); \\ R_{JIK} &= \left(S_{2} \wedge S_{21} \wedge S_{211}\right) \wedge \left(\left(S_{2112} \wedge S_{21122}\right) \vee S_{212}\right). \end{split}$$

С учетом того, что все события на рис. 1 взаимно независимы, для вероятностей  $P_{_{A\!K}},\ P_{_{P\!K}},\ P_{_{D\!K}}$  можно записать

$$\begin{split} P_{_{AK}} &= \boldsymbol{\pi}_{_{1}} + \boldsymbol{\pi}_{_{2}} \cdot \boldsymbol{\pi}_{_{2I}} \cdot \boldsymbol{\pi}_{_{2II}} \cdot \boldsymbol{\pi}_{_{2III}} \cdot \boldsymbol{\pi}_{_{21111}}; \\ P_{_{PK}} &= \boldsymbol{\pi}_{_{2}} \cdot \boldsymbol{\pi}_{_{2I}} \cdot \boldsymbol{\pi}_{_{2II}} \cdot \left(\boldsymbol{\pi}_{_{2111}} \cdot \boldsymbol{\pi}_{_{21112}} + \boldsymbol{\pi}_{_{2112}} \cdot \boldsymbol{\pi}_{_{21121}}\right); \\ P_{_{HK}} &= \boldsymbol{\pi}_{_{2}} \cdot \boldsymbol{\pi}_{_{2I}} \cdot \left(\boldsymbol{\pi}_{_{2II}} \cdot \boldsymbol{\pi}_{_{2112}} \cdot \boldsymbol{\pi}_{_{21122}} + \boldsymbol{\pi}_{_{212}}\right). \end{split}$$

Окончательно имеем

$$P_{AK}^{(1)} = P_1 + (1 - P_1) \cdot (1 - r) \cdot (1 - \beta) \cdot P_2 (1 - r)^{V-1}; \tag{1}$$

$$P_{PK}^{(1)} = (1 - P_1) \cdot (1 - r) \cdot (1 - \beta) \cdot \left\{ P_2 \left[ 1 - (1 - r)^{V-1} \right] + (1 - P_2) \cdot \left[ 1 - r \cdot V \cdot (1 - r)^V \right] \right\}; \tag{2}$$

$$P_{JJK}^{(1)} = (1 - P_1) \cdot (1 - r) \cdot (1 - \beta) \cdot (1 - P_2) \cdot r \cdot V \cdot (1 - r)^V + (1 - P_1) \cdot (1 - r) \cdot \beta. \tag{3}$$

Легко показать, что  $P_{{\scriptscriptstyle AK}}^{(1)} + P_{{\scriptscriptstyle PK}}^{(1)} + P_{{\scriptscriptstyle HK}}^{(1)} + P_{{\scriptscriptstyle HO}}^{(1)} = 1$  .

3.2. Полуавтоматическое исправление ошибок (алгоритм В) внешне (в смысле интерфейса с пользователем) подобно алгоритму Spell-Checker'а текстового редактора (например, Word'a). При отсутствии однозначности корректировки пользователю предлагается для подтверждения до m вариантов исправлений. Если среди них нет правильного варианта, ошибка исправляется вручную. В Word'e предлагаются все установленные возможные варианты исправления, что, впрочем, для определенных классов ошибок тоже не освобождает от полностью ручного исправления.

На рис. 2 приведен фрагмент вероятностно-логического графа алгоритма В, который содержит отличия от алгоритма А.

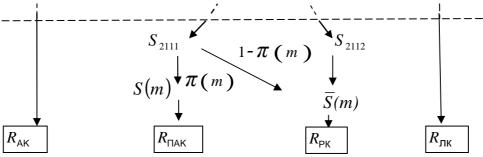


Рис. 2. Фрагмент графа алгоритма полуавтоматического исправления

Здесь приняты следующие дополнительные обозначения:

 $S_m$  и  $\overline{S}_m$  — соответственно ошибка идентифицирована и не идентифицирована среди m синонимов.

Таким образом, имеем следующие вероятностные оценки:

$$P_{AK}^{(2)} = P_1; (4)$$

$$P_{IIAK}^{(2)} = (1 - P_1) \cdot (1 - r) \cdot (1 - \beta) \cdot P_2 \pi(m);$$
(5)

$$P_{PK}^{(2)} = (1 - P_1) \cdot (1 - r) \cdot (1 - \beta) \cdot \{P_2(1 - \pi(m)) + (1 - P_2)\};$$
(6)

$$P_{TK}^{(2)} = (1 - P_1) \cdot (1 - r) \cdot \beta \tag{7}$$

и соответственно  $P_{_{\!A\!K}}^{(2)}+P_{_{\!T\!A\!K}}^{(2)}+P_{_{\!P\!K}}^{(2)}+P_{_{\!T\!K}}^{(2)}+P_{_{\!H\!O}}^{(2)}=1$  .

Вероятность  $\pi(m)$  равна [3]:

$$\pi(m) = \sum_{g=0}^{m-1} C_{V-1}^g \cdot r^g \cdot (1-r)^{V-g-1} + \sum_{g=m}^{V-1} \frac{m}{g+1} C_{V-1}^g \cdot r^g (1-r)^{V-g-1}.$$
 (8)

3.3. Для дополнительной оценки эффективности алгоритмов автоматического и полуавтоматического исправления введем понятие ориентировочной трудоемкости исправления ошибок  $F_{AK}$ ,  $F_{RAK}$ ,  $F_{PK}$  и определим ее как среднее количество операций сравнения и нажатий на клавиши, которые выполняет пользователь при соответствующих финальных исходах. Среднюю трудоемкость F определим как взвешенную сумму:

$$F = P_{AK} F_{AK} + P_{\Pi AK} F_{\Pi AK} + P_{PK} F_{PK}.$$
 (9)

# Алгоритм А

Очевидно,  $F_{AK}^{(A)}=0$  . Далее, предполагая, что при полностью ручном исправлении пользователь в среднем «обрабатывает» половину символов слова, положим  $F_{PK}^{(A)}=n/2$  .

# Алгоритм В

Оценим величины  $F_{PK}^{(B)}$  и  $F_{IJAK}^{(B)}$  для максимального значения m=z, где z – полное количество синонимов. При ручном исправлении пользователю приходится отвергнуть все z синонимов и в среднем обработать  $\frac{n}{2}$  символов, т.е.  $F_{PK}^{(B)}=z+\frac{n}{2}$ , так как в этом случае все синонимы образуются в результате исключительно <u>случайных</u> совпадений:

$$F_{PK}^{(B)} = \sum_{g=0}^{V} gP(g, r, V) + \frac{n}{2} = rV + \frac{n}{2}.$$
 (10)

При полуавтоматическом исправлении ошибка принадлежит  $\mathbf{E}_k^2$ , и, следовательно, один из синонимов заведомо совпадает с T , т.е. является не случайным. Поэтому, с учетом предыдущих рассуждений,

$$F_{\Pi AK}^{(B)} = 1 + \sum_{g=0}^{V-1} \frac{g+2}{2} P(g,r,V) = 1 + \frac{1}{2} r(V-1).$$
 (11)

#### 4. Пример приложения моделей

Рассмотрим результаты приложения моделей к совместному использованию помехоустойчивого удлиненного кода Рида-Соломона [1] и метода анализа обратных вариаций.

Рассматриваемый код является одним из кодов над полем Галуа  $\mathit{GF}(p^{^m})$  , где p – целое.

Длина кода  $n_{_{\!\scriptscriptstyle H}}+n_{_{\!\scriptscriptstyle L}}=p+1, \;\; n_{_{\!\scriptscriptstyle L}}=2$  .

В примере, приведенном в [1] для иллюстрации алгоритмов формирования и декодирования кода, p=11, исходное информационное слово  $A_n=250000001$ ; контрольные символы  $a_{01}=3, a_{02}=0$ ; закодированное слово  $A_{n=n\,k}=25000000130$ . Здесь значения информационных символов подобраны так, чтобы при вычислении избыточных символов не выйти за пределы десятичного алфавита. В общем случае, конечно, избыточные символы могут принимать одно из p значений и, следовательно, должны представляться (или могут интерпретироваться) как числа в системе счисления с основанием p. В данном примере это должно быть 11-ричное (или 16-ричное) основание. В связи с этим отметим, что двухразрядное число в системе счисления с основанием  $p \le 33$  можно представить трехразрядным десятичным числом, т.к.  $33^2 < 10^3 < 34^2$ . Поэтому для  $p \le 33$  два избыточных символа в алфавите p можно заменить тремя десятичными цифрами. Например, для p = 11, пару значений  $\alpha_{01} = 10$  и  $\alpha_{02} = 07$  можно интерпретировать как двухразрядное 11-ричное число 10/07, десятичный эквивалент которого равен 117. Таким образом, для цифрового кода q = 10 может быть принято q = 31 при трех реальных избыточных символах и двух виртуальных (при соответствующем усложнении алгоритмов декодирования). Аналогичные рассуждения применимы и к другим q, p.

Описанный код полностью обнаруживает и исправляет однократные транскрипции.

Примем  $E = \{E_1, E_2, E_3, E_4, E_5, E_6\}$ ; смысл классов ошибок и значений связанных с ними параметров приведен в табл. 1.

Таблица 1. Классы ошибок

| Класс<br>ошибок | Характер ошибок                | Вероятность<br>появления, | Количество<br>генерируемых вариаций |
|-----------------|--------------------------------|---------------------------|-------------------------------------|
| $E_{i}$         |                                | $p_i$ [4]                 |                                     |
| $E_1$           | Однократные транскрипции       | 0,5557                    | $(q-1)\cdot n$                      |
| $E_2$           | Вставка символа                | 0,1567                    | n                                   |
| $E_3$           | Выпадение символа              | 0,1204                    | $q \cdot (n+1)$                     |
| $E_4$           | Транспозиция соседних симвопов | 0,0664                    | n-1                                 |
| $E_5$           | Двукратные транскрипции        | 0,0322                    | $(q-1)^2 \cdot C_n^2 - n + 1$       |
| $E_6$           | Многократные ошибки            | 0,0686                    | _                                   |

Для рассматриваемого кода  $\mathbf{E}_k^1 = \left\{E_1\right\}, \mathbf{E}_k^2 = \left\{E_i\right\}.$ 

Результаты иллюстративных расчетов для моделей автоматического (алгоритм A) и полуавтоматического (алгоритм B) исправления приведены в табл. 2 и 3 соответственно. Сводная таблица результатов, отражающая вероятностные характеристики вариантов декодирования и соответствующие показатели трудоемкости для значения r=0,001, q=37, n=10, приведена в табл. 4. В данных табл. 4 учтено, что для варианта декодирования, ограниченного рассматриваемым кодом, как видно из рис. 1,  $P_{AK}=P_1$ ;  $P_{PK}=1-P_1$ ;  $P_{PK}=(1-P_1)(1-r)(1-\beta)$ ;

$$P_{JJK} = (1 - P_1)(1 - r)\beta; F = P_{PK} \frac{n}{2}.$$

При расчетах принято  $\mathbf{E}_k^{21} = \{E_4\}$ ;  $\mathbf{E}_k^{22} = \{E_2, E_3, E_4\}$ ;  $\boldsymbol{\beta} = r$  при допущении о псевдослучайном характере распределения результатов декодирования кода, искаженного ошибкой, не принадлежащей к  $\mathbf{E}_k^1 = \{E_1\}$ .

Таблица 2. Иллюстративные расчеты для алгоритма А

| 2                   | $r = 0.001, \ q = 10, \ n = 10$ |          |                   | $r = 0.001, \ q = 37, \ n = 10$ |          |               |  |
|---------------------|---------------------------------|----------|-------------------|---------------------------------|----------|---------------|--|
| $\mathbf{E}_k^2$    | $P_{AK}$                        | $P_{PK}$ | $P_{{\it J\! K}}$ | $P_{{\scriptscriptstyle AK}}$   | $P_{PK}$ | $P_{J\!I\!K}$ |  |
| $\mathbf{E}_k^{21}$ | 0,62144                         | 0,37431  | 0,0038077         | 0,62144                         | 0,37431  | 0,0038077     |  |
| $\mathbf{E}_k^{22}$ | 0,85731                         | 0,13040  | 0,011850          | 0,77977                         | 0,19136  | 0,028427      |  |

Таблица 3. Иллюстративные расчеты для алгоритма В

|   | $\mathbf{E}_k^2$    | $P_{AK}=0,$                     | 55570, $P_{JK} =$           | = 0,001, | $P_{AK} = 0.55570, \ P_{JJK} = 0.001,$ |                             |          |  |
|---|---------------------|---------------------------------|-----------------------------|----------|----------------------------------------|-----------------------------|----------|--|
| m |                     | $r = 0.001, \ q = 10, \ n = 10$ |                             |          | $r = 0.001, \ q = 37, \ n = 10$        |                             |          |  |
|   |                     | $P_{\it \Pi AK}$                | $P_{\scriptscriptstyle PK}$ | $\pi(m)$ | $P_{\it \Pi AK}$                       | $P_{\scriptscriptstyle PK}$ | $\pi(m)$ |  |
| 1 | $\mathbf{E}_k^{21}$ | 0,066003                        | 0,37741                     | 0,99601  | 0,066003                               | 0,37741                     | 0,99601  |  |
|   | $\mathbf{E}_k^{22}$ | 0,32177                         | 0,12164                     | 0,93863  | 0,27926                                | 0,16415                     | 0,81461  |  |
|   | $\mathbf{E}_k^{21}$ | 0,066267                        | 0,37715                     | 0,99999  | 0,066267                               | 0,37715                     | 0,99999  |  |
| 2 | $\mathbf{E}_k^{22}$ | 0,34194                         | 0,10147                     | 0,99746  | 0,33444                                | 0,10897                     | 0,97558  |  |
|   | $\mathbf{E}_k^{21}$ | 0,066267                        | 0,37714                     | 1,0000   | 0,066267                               | 0,37714                     | 1,0000   |  |
| 4 | $\mathbf{E}_k^{22}$ | 0,34281                         | 0,10060                     | 1,0000   | 0,34274                                | 0,10067                     | 0,99980  |  |
| Z | $\mathbf{E}_k^{21}$ | 0,066267                        | 0,37714                     | 1,0000   | 0,066267                               | 0,37714                     | 1,0000   |  |
| L | $\mathbf{E}_k^{22}$ | 0,34289                         | 0,10060                     | 1,0000   | 0,34282                                | 0,10060                     | 1,0000   |  |

Таблица 4. Сводные характеристики алгоритмов

| Алгоритм<br>декодирования | $\mathbf{E}_k^2$    | $P_{AK}$ | $P_{\it \Pi AK}$ | $P_{PK}$ | $P_{_{\it JIK}}$ | F    |
|---------------------------|---------------------|----------|------------------|----------|------------------|------|
| Код                       |                     | 0,5557   | _                | 0,4434   | 0,0004           | 2,22 |
| Vод I одгоритм A          | $\mathbf{E}_k^{21}$ | 0,6214   | -                | 0,3743   | 0,0038           | 1,87 |
| Код+ алгоритм А           | $\mathbf{E}_k^{22}$ | 0,7797   | _                | 01913    | 0,0284           | 0,96 |
| Vод годгориты В           | $\mathbf{E}_k^{21}$ | 0,5557   | 0,6626           | 0,3771   | 0,0004           | 1,95 |
| Код+алгоритм В            | $\mathbf{E}_k^{22}$ | 0,5557   | 0,3428           | 0,1006   | 0,0004           | 0,96 |

### 5. Анализ данных

1. Как видно из данных табл. 2, 4, комбинированная процедура декодирования анализом вариаций ошибочного слова и автоматическим исправлением по виртуальному словарю позволяет повысить относительное количество исправляемых ошибок и снизить трудоемкость ввода. Так, в зависимости от выбранного множества  $\mathbf{E}_k^2$ , значение  $P_{AK}$  может быть повышено от 0,5557 до 0,7797 и более.

Соответственно значение показателя трудоемкости F может быть уменьшено с 2,22 до 0,96. Однако при этом повышается относительное количество ложно корректируемых ошибок. Хотя окончательное решение относительно приемлемости цены (увеличение  $P_{JK}$ ), которую стоит платить за снижение F, остается за проектировщиком, можно предположить, что практически использование алгоритма A может иметь смысл лишь для режима off-line, когда подтверждение исправления затруднено.

- 2. Для полуавтоматического исправления (табл. 3, 4) доля ложно корректируемых ошибок не увеличивается, а значение показателя суммарной трудоемкости F существенно снижается по сравнению с чисто кодовой процедурой декодирования и исправления. При этом снижение трудоемкости тем больше, чем больше классов ошибок включено в  $E_k^2$ . Поэтому может оказаться целесообразным дополнение  $\mathbf{E}_k^2$  двукратными транскрипциями и/или специфическими ошибками иных классов, выходящих за рамки упрощенного перечня табл. 1.
- 3. Сделанные заключения базируются на количественных результатах применения кода Рида-Соломона ( $\mathbf{E}_k^1 = \{E_1\}$ ), однако они качественно не меняются и при применении других кодов, например, [5] ( $\mathbf{E}_k^1 = \{E_1, E_4\}$ ).

#### 6. Выводы

Дополнение помехозащитного кода с исправлением ошибок методом корректировки по виртуальному словарю допустимых слов позволяет улучшить корректирующие и трудоемкостные характеристики кода. Полученные соотношения (1) – (3) и (4) – (7) позволяют получить ориентировочные оценки, характеризующие результаты применения метода в зависимости от заданных условий и используемого алгоритма и принять соответствующие решения.

Рассмотренный подход может оказаться полезным при выборе решения о корректировке ошибок каналов связи и носителей информации.

# СПИСОК ЛИТЕРАТУРЫ

- 1. Бояринов И.М., Давыдов А.А. Мамедли Э.М., Смеркис Ю.Б. Использование помехоустойчивого кодирования для защиты информации от ошибок оператора // АТ. 1983. № 2. С. 5–48.
- 2. Кузьменко Г.Є., Литвинов В.А., Майстренко С.Я., Ходак В.І. Алгоритми і моделі автоматичної ідентифікації та корекції типових помилок користувача на основі природної надмірності // Математичні машини і системи. 2004. № 2. С. 134–148.
- 3. Литвинов В.А., Майстренко С.Я., Ступак Н.Б. Некоторые оценки вероятностных характеристик процесса автоматической идентификации ошибок пользователя на основе эталонного словаря // УСиМ. 2001. № 2. С. 21–24.
- 4. Литвинов В.А., Крамаренко В.В. Контроль достоверности и восстановления информации в человекомашинных системах. Киев: Техніка, 1986. 200 с.
- 5. Sethi A.S., Rajaraman V., Kenjale P.S. An error-correcting coding shame for alphanumeric data # Information Processing Letters. 1988. Vol. 7. P. 72–77.