ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ БЕЛАРУСЬ

СТБ ISO/IEC 7064/*OP*

Информационные технологии

Методы защиты

СИСТЕМЫ КОНТРОЛЬНЫХ ЗНАКОВ

Інфармацыйныя тэхналогіі

Метады абароны

СІСТЭМЫ КАНТРОЛЬНЫХ ЗНАКАЎ

(ISO/IEC 7064:2003, IDT)

Издание официальное

Госстандарт

Минск

УДК 004.223.3.056 (083.74)(476) МКС 35.240.40 КП 05 IDT

Ключевые слова: контрольный знак, модуль, конгруэнтность, чистые системы, гибридные системы, рекурсивный метод, метод полиномов, строка

Предисловие

Цели, основные принципы, положения по государственному регулированию и управлению в области технического нормирования и стандартизации установлены Законом Республики Беларусь «О техническом нормировании и стандартизации».

1 ПОДГОТОВЛЕН Расчетным центром Национального банка Республики Беларусь
ВНЕСЕН Национальным банком Республики Беларусь

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Госстандарта Республики Беларусь от 28 августа 2015 г. № 38

3 Настоящий стандарт идентичен международному стандарту ISO/IEC 7064:2003 Information technology – Security techniques – Check character systems (Информационные технологии. Методы защиты. Системы контрольных знаков).

Международный стандарт разработан подкомитетом SC 27 «Методы защиты в IT-сфере» объединенного технического комитета по стандартизации ISO/IEC JTC 1 «Информационные технологии» Международной организации по стандартизации (ISO) и Международной электротехнической комиссии (IEC).

Перевод с английского языка (en).

Официальный экземпляр международного стандарта, на основе которого подготовлен настоящий государственный стандарт, имеется в Национальном фонде ТНПА.

Степень соответствия – идентичная (IDT)

4 ВВЕДЕН ВПЕРВЫЕ

Издан на русском языке

Содержание

Введение

Необходимость стандартизации систем контрольных знаков определяется следующими соображениями:

a) многие системы из множества используемых систем имеют очень схожие характеристики, причем большая часть вариантов не дает никаких преимуществ;

b) некоторые из существующих систем были тщательно проверены математическими методами и некоторые из них имеют серьезные недостатки;

c) разнообразие систем подрывает экономические характеристики продуктов, которые генерируют или проверяют достоверность контрольных знаков, а также часто препятствует проверке обмена данными.

В связи с этим выбран небольшой набор совместимых систем, удовлетворяющих требованиям различных приложений; они были проверены на достоверность и в рамках ограничений каждого приложения обеспечивают высокую защиту от типичных ошибок при записи и вводе данных.

Существующие системы контрольных знаков, описанные в ISO 2108, ISO 2894 и ISO 6166, используются в конкретных областях применения (ISO 2894 был отозван). Однако им не удалось достичь такого уровня обнаружения ошибок, как в системах, указанных в настоящем стандарте.

В приложении A обобщены критерии, которые необходимо учитывать при выборе системы контрольных знаков, указанной в настоящем стандарте, для конкретного применения.

Приложение B содержит описание метода, позволяющего применять настоящий стандарт к алфавиту, содержащему более 26 символов.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ БЕЛАРУСЬ

Информационные технологии
Методы защиты
СИСТЕМЫ КОНТРОЛЬНЫХ ЗНАКОВ

Інфармацыйныя тэхналогіі
Метады абароны
СІСТЭМЫ КАНТРОЛЬНЫХ ЗНАКАЎ

Information technology
Security techniques
Check character systems

Дата введения 2016-03-01

1 Область применения

1.1 Настоящий стандарт устанавливает набор систем контрольных знаков, предназначенных для защиты строк от ошибок, которые возникают при копировании или наборе данных. Строки могут быть фиксированной или переменной длины, а также содержать наборы символов, которые могут быть:

a) цифровыми (10 цифр: от 0 до 9);

b) буквенными (26 букв: от A до Z);

c) буквенно-цифровыми (буквы и цифры).

Встроенные пробелы и специальные символы игнорируются.

1.2 Настоящий стандарт устанавливает требования соответствия для продуктов, описанных как генерирующие контрольные знаки или проверяющие строки с использованием систем, приведенных в настоящем стандарте.

1.3 Данные системы контрольных знаков могут обнаруживать:

a) все единичные ошибки замещения символов (замещение одного символа другим, например «4234» вместо «1234»);

b) все или почти все единичные (локальные) ошибки перестановки (перестановка двух отдельных знаков, стоящих рядом или с одним знаком между ними, например «12354» или «12543» вместо «12345»);

c) все или почти все ошибки циклического сдвига (циклические сдвиги целой строки влево или вправо);

d) высокую долю ошибок двойного замещения (две отдельные ошибки замещения в одной и той же строке, например «72345887» вместо «12345667»);

e) высокую долю других ошибок.

1.4 Настоящий стандарт не распространяется на системы, разработанные исключительно для:

a) обнаружения ошибок и автоматического исправления;

b) выявления преднамеренной фальсификации;

c) проверки строк, обмен которыми осуществлен только между машинами.

1.5 Настоящий стандарт предназначен для использования при обмене информацией между организациями. Кроме того, настоятельно рекомендуется использовать настоящий стандарт во внутренних информационных системах.

2 Термины и определения

В настоящем стандарте применяют следующие термины с соответствующими определениями:

2.1 контрольный знак (check character): Добавленный знак, который может использоваться для проверки верности строки по математическому отношению к этой строке.

2.2 система контрольных знаков (check character system): Набор правил для генерации контрольных знаков и проверки строк, включающих контрольные знаки.

Издание официальное

2.3 дополнительный контрольный знак (supplementary check character): Контрольный знак, который не принадлежит к набору знаков тех строк, которые должны быть защищены.

2.4 модуль (modulus): Целое число, которое используется в качестве делителя целочисленного делимого для получения целочисленного остатка.

2.5 конгруэнтность (congruence): Свойство некоторого набора целых чисел, которые отличаются друг от друга величиной, кратной модулю. Конгруэнтность обозначается символом «Ξ». Например, 39 Ξ 6 (mod 11) показывает, что 39 и 6 конгруэнтны по отношению к модулю 11, т. е. 39 − 6 = 33, которое кратно 11.

2.6 основание системы счисления (radix): Знаменатель геометрической прогрессии.

3 Символы и обозначения

В настоящем стандарте применяют следующие символы и обозначения:

α_i – численное значение символа в положении i;

i – индекс позиции символа;

M – модуль;

n – количество символов в строке, включая контрольный знак;

P_i, S_i, V – целые числа, которые используются при вычислении контрольного знака для хранения промежуточного результата;

r – основание системы счисления;

w_j – весовое значение для метода полиномов;

X, * – дополнительные контрольные знаки;

:= – символ, обозначающий операцию «установить равным», используемую в процедурных спецификациях контрольных знаков, указывающий, что значение целого числа на левой стороне символа должно быть равно значению выражения на правой стороне символа;

Ξ – символ, обозначающий «конгруэнтность» (см. 2.5);

$|\,|_M$ – символ, обозначающий уникальное целое число между 1 и M, которое является остатком после деления на M; если этот остаток равен нулю, то заменяется на значение M;

$|_{M+1}$ – символ, обозначающий уникальное целое число между 0 и M, которое является остатком после деления на $M + 1$; остаток после этой операции никогда не равняется нулю;

(mod M) – символ, обозначающий уникальное целое число между 0 и $M − 1$, которое является остатком после деления на M.

4 Типы систем

В настоящем стандарте определяется два типа систем:

a) чистые системы (см. разделы 6–8);

b) гибридные системы (см. разделы 9, 10).

4.1 Чистые системы

Чистые системы приведены в таблице 1 и описаны в разделах 6–8. Каждая из них использует единый модуль для всех этапов расчета.

4.2 Гибридные системы

Гибридные системы приведены в таблице 2 и описаны в разделах 9 и 10. Каждая из гибридных систем использует два модуля в расчетах. Один модуль равен, а второй больше, чем число символов в наборе символов защищаемой строки. Эти гибридные системы всегда предусматривают контрольные знаки в наборе символов защищаемой строки.

5 Соответствие и обозначение

5.1 Строки

Строки, защищенные одной из систем, указанных в настоящем стандарте для соответствующего применения, соответствуют требованиям настоящего стандарта.

5.2 Продукты, генерирующие контрольные знаки

5.2.1 Продукты (реализованные программными или аппаратными средствами), которые описаны как генерирующие контрольные знаки по настоящему стандарту без дополнительного уточнения,

должны быть способны генерировать контрольные знаки для всех систем, описанных в настоящем стандарте.

5.2.2 В описании продуктов, которые генерируют контрольные знаки не для всех систем, указанных в настоящем стандарте, должны указываться те системы, которые они охватывают, например «генерирует контрольные знаки в соответствии с ISO/IEC 7064, MOD 11-2».

5.3 Контролирующие продукты

5.3.1 Продукты (реализованные программными или аппаратными средствами), которые описаны как контролирующие строки без дополнительного уточнения, должны подходить для использования всех систем, описанных в настоящем стандарте.

5.3.2 В описании продуктов, которые проверяют строки с использованием только некоторых из систем, описанных в настоящем стандарте, должны указываться те системы, которые они охватывают, например «проверяет строки с использованием ISO/IEC 7064, MOD 11-2».

5.4 Обозначение системы

5.4.1 Как правило, требуется использовать полное обозначение каждой системы, которое приведено в таблицах 1 и 2, например «ISO/IEC 7064, MOD 11-2».

Примечание – Сокращенные формы, такие как MOD 11, могут привести к путанице с аналогичными системами, использующими модуль 11.

Таблица 1 – Чистые системы

Обозначение системы контрольного знака [1)]	Применение	Количество и тип контрольных знаков [2)]
ISO/IEC 7064, MOD 11-2	Цифровые строки	1 цифра или дополнительный контрольный знак «X»
ISO/IEC 7064, MOD 37-2	Буквенно-цифровые строки	1 цифра, или буква, или дополнительный контрольный знак «*»
ISO/IEC 7064, MOD 97-10	Цифровые строки	2 цифры
ISO/IEC 7064, MOD 661-26	Буквенные строки	2 буквы
ISO/IEC 7064, MOD 1271-36	Буквенно-цифровые строки	2 цифры или буквы
[1)] Первое число после «MOD» в обозначении является модулем, а второе – основанием системы счисления. [2)] Первые две системы могут дать дополнительный контрольный знак вне набора символов строки, которую нужно проверить (т. е. контрольные знаки в ISO/IEC 7064, MOD 11-2 – это символы от «0» до «9» плюс «X», а контрольные знаки в ISO/IEC 7064, MOD 37-2 – это символы от «0» до «9», от «A» до «Z», а также «*»). Если дополнительный контрольный знак неприемлем и требуется один контрольный знак, то можно избежать выдачи тех строк, которые дают дополнительный контрольный знак. Если дополнительный контрольный знак недопустим и невозможно избежать строк, которые его генерируют, рекомендуется использовать гибридные системы.		

Таблица 2 – Гибридные системы

Обозначение системы контрольного знака [1)]	Применение	Количество и тип контрольных знаков
ISO/IEC 7064, MOD 11,10	Цифровые строки	1 цифра
ISO/IEC 7064, MOD 27,26	Буквенные строки	1 буква
ISO/IEC 7064, MOD 37,36	Буквенно-цифровые строки	1 цифра или буква
[1)] Два числа после «MOD» в обозначении – два модуля.		

5.4.2 Если имеется особая потребность в краткости, например когда необходимо сопровождать передаваемый элемент данных указанием системы, используемой для его защиты, могут использоваться одноразрядные цифровые обозначения, указанные в таблице 3.

Таблица 3 – Одноразрядные обозначения

Система контрольных знаков	Обозначение
ISO/IEC 7064, MOD 11-2	1
ISO/IEC 7064, MOD 37-2	2
ISO/IEC 7064, MOD 97-10	3
ISO/IEC 7064, MOD 661-26	4

Окончание таблицы 3

Система контрольных знаков	Обозначение
ISO/IEC 7064, MOD 1271-36	5
ISO/IEC 7064, MOD 11,10	6
ISO/IEC 7064, MOD 27,26	7
ISO/IEC 7064, MOD 37,36	8
Нет контрольного знака или нестандартная система	0

6 Спецификация чистых систем

6.1 Формула

Символьная строка удовлетворяет проверке, если:

$$\sum_{i=1}^{n} \alpha_i \cdot r^{i-1} \equiv 1 \pmod{M},$$

где n – количество символов в строке, включая контрольный (ые) знак (и);
i – индекс позиции символа начиная справа (т. е. для крайнего правого символа $i = 1$) без учета пробелов и специальных знаков;
α_i – значение символа в позиции i, как определено в таблице 4;
r – основание системы счисления (т. е. знаменатель геометрической прогрессии);
M – модуль.

6.2 Расчет

Можно применять любую методику расчета, которая удовлетворяет формуле.

6.3 Позиция контрольного знака

Контрольный (ые) знак (и) должен (ы) помещаться в крайнем правом конце строки.

7 Методы расчета для чистых систем с одним контрольным знаком

В настоящем стандарте определяется два основных вычислительных метода для чистых систем: рекурсивный метод и метод полиномов. Оба метода дают одинаковый результат и требуют одинакового количества операций умножения и сложения. Метод полиномов требует больше памяти, так как нужно сохранять весовые значения системы.

7.1 Рекурсивный метод чистых систем

7.1.1 Расчет

В рекурсивном методе строка обрабатывается знак за знаком слева направо.

Алгоритм генерирования контрольного знака α_1 можно описать следующим образом.

При индексе $j = 1 \ldots (n - 1)$, где n – количество символов в строке, включая контрольный знак, и принимая $P_j = 0$ для $j = 1$, получают:

$$S_j := P_j + \alpha_{n-j+1};$$

$$P_{j+1} := S_j \cdot r,$$

где α_{n-j+1} – значение символа;
r – основание системы счисления.

Следующее значение a_1 выбирается таким, чтобы

$$P_n + \alpha_1 \equiv 1 \pmod{M}$$

или

$$a_1 := (1 - P_n) \pmod{M}.$$

Алгоритм проверки правильности контрольного знака α_1 можно описать следующим образом.

При индексе $j = 1 \ldots n$, где n – количество символов в строке, включая контрольный знак, и принимая $P_j = 0$ для $j = 1$, получают:

$$S_j := P_j + a_{n-j+1};$$

$$P_{j+1} := S_j \cdot r.$$

Строка считается верной, если

$$S_n \equiv 1 \pmod{M}.$$

Альтернативным образом процедуру получения контрольного знака α_1 можно повторить. Строка считается верной, если сгенерированный контрольный знак соответствует существующему знаку α_1.

Таблица 4 – Значения, присвоенные символам

Символ	Значения в системах для цифровых строк	Значения в системах для буквенных строк	Значения в системах для буквенно-цифровых строк
0	0		0
1	1		1
2	2		2
3	3		3
4	4		4
5	5		5
6	6		6
7	7		7
8	8		8
9	9		9
X [1)]	10		
A		0	10
B		1	11
C		2	12
D		3	13
E		4	14
F		5	15
G		6	16
H		7	17
I		8	18
J		9	19
K		10	20
L		11	21
M		12	22
N		13	23
O		14	24
P		15	25
Q		16	26
R		17	27
S		18	28
T		19	29
U		20	30
V		21	31
W		22	32
X		23	33
Y		24	34
Z		25	35
* [2)]			36

[1)] Для ISO/IEC 7064 MOD 11-2.
[2)] Для ISO/IEC 7064 MOD 37-2.

7.1.2 Пример

Предположим, что в строку «0794» требуется добавить контрольный знак с использованием системы контрольных знаков ISO/IEC 7064, MOD 11-2.

Здесь $M = 11$, $r = 2$ и $n = 5$ (т. е. 4 символа плюс 1 контрольный знак).

После этого выполняется расчет, как указано в таблице 5.

В этом примере конечное значение P_n равно 100. Данное значение плюс контрольный знак должно быть конгруэнтено 1 (mod 11). Поскольку число 100 само по себе конгруэнтно 1 (mod 11), то значение контрольного знака должно быть равно нулю, а полностью защищенная строка – «0794<u>0</u>», так как контрольный знак добавляется к строке справа.

Чтобы проверить строку, нужно выполнить указанные выше шаги j = от 1 до 5, как показано, но со значением контрольного знака, равным 0, включенным в расчет; если результат конгруэнтен 1 (mod 11), то строка считается верной.

Примечания

1 Если на каком-либо этапе произведение P_{j+1} или сумма S_j больше значения модуля M, то кратными числами этого модуля можно пренебречь, а целочисленный остаток использовать для дальнейших расчетов. В расчетах в таблице 5:

$P_3 = 14$, но может быть $14 - 11 = 3$
$S_3 = 23$, но может быть $23 - 22 = 1$
$P_4 = 46$, но может быть $46 - 44 = 2$

2 Действительными значениями контрольных знаков в системе ISO/IEC 7064, MOD 11-2 являются 0–10. Если значение контрольного знака равно 10, то он представляется дополнительным контрольным знаком «X». Если исходная строка была короче «079», то в конце шага 3 значение будет 46:

$$46 \equiv 2 \pmod{11},$$

поскольку $2 + 10 \equiv 1 \pmod{11}$, полная строка равна «079<u>X</u>».

Чтобы проверить строку, после шага 3 выполняют сложение (46 + 10 = 56) и получают значение, которое конгруэнтно 1 (mod 11), следовательно, строка удовлетворяет критериям проверки.

7.2 Метод полиномов для чистых систем

7.2.1 Расчет

Метод полиномов для чистых систем рассчитывается путем умножения значения для каждого символа в строке на r^{i-1} или $r^{i-1} \pmod{M}$, который обозначается весовым значением w_i. Список первых пятнадцати значений $r^{i-1} \pmod{M}$ для всех чистых систем приведен в таблице 6.

Умножают значения символов на их весовые значения, а затем прибавляют произведения. Строки, включающие контрольный знак, действительны, если сумма этих произведений конгруэнтна 1 (mod M).

7.2.2 Пример

Расчет для генерирования контрольного знака по методу полиномов строки, используемой в 7.1.2, т. е. «0794», – это:

Позиция символа i:	5	4	3	2	1
Весовое значение $2^{i-1} \pmod{11}$	5	8	4	2	1
Значение символа α_i	0	7	9	4	
Произведения	0	56	36	8	

Сумма произведений $0 + 56 + 36 + 8 = 100$

Сумма, которая в данном случае равна 100, плюс контрольный знак должна быть конгруэнтной 1 (mod 11). Поскольку число 100 само по себе конгруэнтно 1 (mod 11), то значение контрольного знака должно быть равно нулю, а полная защищенная строка – «0794<u>0</u>». Следует обратить внимание на то, что контрольный знак добавляется к строке справа.

Чтобы проверить строку с помощью этого метода, умножают значение каждого символа (включая значение контрольного знака) на весовое значение, связанное с его позицией; складывают произведения и делят на 11, чтобы получить остаток. Если остаток равен 1, проверка выполнена. Расчет для проверки полной защищенной строки:

Позиция символа i:	5	4	3	2	1
Весовое значение $2^{i-1} \pmod{11}$	5	8	4	2	1
Значение символа α_i	0	7	9	4	0
Произведения	0	56	36	8	0

Сумма произведений 0 + 56 + 36 + 8 = 100
Ξ 1 (mod 11)

соответственно, удовлетворяет критериям проверки.

Примечание – Правая позиция, т. е. позиция с весовым значением r = 1, зарезервирована для контрольного знака, поэтому правая позиция исходной строки (без контрольного знака) связана с весовым значением r, в данном случае 2.

Таблица 5 – Пример рекурсивного метода для чистых систем

Шаг	Произведение, перенесенное вперед	+	Значение следующего знака	=	Промежуточная сумма (см. 7.1.2, примечание 1)	Промежуточная сумма	×	Основание системы счисления	=	Произведение, перенесенное вперед (см. 7.1.2, примечание 1)
j	P_j	+	α_{n-j+1}	=	S_j	S_i	×	r	=	P_{j+1}
1	0	+	0	=	0	0	×	2	=	0
2	0	+	7	=	7	7	×	2	=	14
3	14	+	9	=	23	23	×	2	=	46
4	46	+	4	=	50	50	×	2	=	100
5	100	+	контрольный знак (должен быть конгруэнтен 1 (mod 11))							

Таблица 6 – Весовые значения для чистой системы

Индекс позиции	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
ISO/IEC 7064, MOD 11-2	5	8	4	2	1	6	3	7	9	10	5	8	4	2	1
ISO/IEC 7064, MOD 37-2	30	15	26	13	25	31	34	17	27	32	16	8	4	2	1
ISO/IEC 7064, MOD 97-10	53	15	50	5	49	34	81	76	27	90	9	30	3	10	1
ISO/IEC 7064, MOD 661-26	129	488	273	341	547	199	389	498	70	562	225	390	15	26	1
ISO/IEC 7064, MOD 1271-36	769	904	590	87	532	156	428	718	373	893	625	900	25	36	1

Примечание – Весовые значения показаны только для первых пятнадцати позиций. Серии можно продлевать бесконечно, используя формулу $w_i := r^{i-1} \pmod M$, где w_i является весовым значением для позиции i.

8 Методы расчета для чистых систем с двумя контрольными знаками

8.1 Расчет

Расчет контрольных знаков для этих систем осуществляется так же, как в системах с одним контрольным знаком, до заключительного этапа, когда в системах с основанием, отличным от 10, требуется дополнительный шаг, чтобы извлечь два значения символов для контрольных знаков. (Сведения о системе контрольных знаков ISO/IEC 7064, MOD 97-10 приведены в 8.4.) Обозначают результат, получаемый до заключительного этапа, буквой V. Два значения контрольных знаков можно найти путем деления результата V на основание r. Целое частное – это значение контрольного знака для позиции i = 2, а остаток – это значение контрольного знака для позиции i = 1 или

$$\alpha_1 := V \pmod r;$$

$$\alpha_2 := (V - \alpha_1) / r.$$

8.2 Пример с использованием рекурсивного метода

Чтобы вычислить два контрольных знака для строки «ISO 79» с использованием системы ISO/IEC 7064, MOD 1271-36, рекурсивным методом с использованием значений буквенно-цифровых символов, приведенных в таблице 4, выполняются шаги 1–6, указанные в таблице 7. Следует обратить внимание на то, что встроенный пробел игнорируется, как указано в 1.1.

Заключительный шаг (шаг 7) – расчет контрольного значения – состоит из вычитания последнего $P_{j+1} \pmod M$ из M + 1. Следовательно,

$$1271 + 1 = 1272,$$

$$\text{тогда } 1272 - 1132 = 140.$$

Чтобы получить отдельные значения символов, которые составляют V = 140, делят это значение на основание системы счисления 36; это дает частное 3 и остаток 32.

Частное 3 является значением контрольного знака в позиции (i = 2), а остаток 32 является значением контрольного знака в позиции (i = 1). Используя значения символов из таблицы 4, которые соответствуют значениям 3 и W, получают полную защищенную строку «ISO 793W».

Чтобы проверить эту строку, следует выполнить шаги 1–5 точно так, как показано выше, а шаги 6 и 7 – так, как указано в таблице 8:

$1272 \equiv 1 \pmod{1271}$, тем самым удовлетворяя критериям проверки.

Таблица 7 – Пример чистого рекурсивного метода с двумя контрольными знаками

Шаг	Произведение, перенесенное вперед	+	Значение следующего знака	=	Промежуточная сумма	Промежуточная сумма	×	Основание	=	Произведение	Произведение (mod 1271), перенесенное вперед
j	P_j	+	α_{n-j+1}	=	S_j	S_i	×	r	=	P_{j+1}	P_{j+1} (mod M)
1	0	+	18	=	18	18	×	36	=	648	648
2	648	+	28	=	676	676	×	36	=	24336	187
3	187	+	24	=	211	211	×	36	=	7596	1241
4	1241	+	7	=	1248	1248	×	36	=	44928	443
5	443	+	9	=	452	452	×	36	=	16272	1020
6	1020	+	0 [1)]	=	1020	1020	×	36	=	36720	1132

[1)] Поскольку позиция, занимаемая первым контрольным знаком, на этом этапе все еще пуста, ее значение равно нулю.

Таблица 8 – Пример проверки достоверности для чистого рекурсивного метода с двумя контрольными знаками

6	1020 + 3 = 1023	1023 × 36 = 36828	1240 (mod 1271)
7	1240 + 32 = 1272	(см. *)	

$1272 \equiv 1 \pmod{1271}$, тем самым удовлетворяя критериям проверки.

* Последнее значение символа просто прибавляется, а полученная сумма не умножается на основание.

8.3 Пример с использованием метода полиномов

Процедура вычисления двух контрольных знаков для примера из 7.2, строка «ISO 79» при помощи метода полиномов с использованием весовых значений из таблицы 4 и значений символов из таблицы 6 указываются в таблице 9. Затем следует процедура, описанная в 8.2 (шаг 7), что в результате дает «ISO 793W».

8.4 Упрощенная процедура для ISO/IEC 7064, MOD 97-10

Для этой системы следует выполнять процедуры, описанные в 8.2 и 8.3.

Однако поскольку в нормальной десятичной системе счисления цифры уже взвешены по степеням основания 10, можно применять упрощенную процедуру. Для этого добавляют к строке два нуля и делят на 97. Вычитают полученный остаток из 98. Две цифры в результате являются значениями контрольных знаков.

Для строки «794» применяется следующая процедура:

– шаг 1: добавить два нуля в позиции контрольных знаков: 79400;

– шаг 2: разделить на 97, что дает частное 818 и остаток 54;

– шаг 3: определить значение контрольного знака как (97 + 1) − 54 = 44 и добавить его к исходной строке, чтобы получить 79444.

Для проверки делят строку на 97, если остаток равен 1, критерий проверки удовлетворен.

Таблица 9 – Пример метода полиномов с двумя контрольными знаками

Позиция символа i:	7	6	5	4	3	2	1
Весовое значение w_i (mod 11)	373	893	625	900	25	36	1
Значение символа α_i	18	28	24	7	9		
Произведения	6714	25004	15000	6300	225		
Сумма произведений	6714	+ 25004	+ 15000	+ 6300	+ 225	= 53243	
						= 1132 (mod 1271)	

9 Спецификация гибридных систем

9.1 Формула

Для гибридных систем количество символов M в наборе символов должно быть четным.

Строка символов, включающая контрольный знак, сгенерированная по стандартной гибридной формуле, удовлетворяет проверке, если

$$(\ldots((((M + \alpha_n) \|_M \cdot 2) |_{M+1} + \alpha_{n-1}) \|_M \cdot 2) |_{M+1} + \ldots + \alpha_1) \|_M = 1,$$

где n – количество символов в строке, включая контрольный знак;

i – индекс позиции символа, считая справа (т. е. для крайнего правого символа $i = 1$), без учета пробелов и специальных знаков;

α_i – значение символа в позиции i, как определено в таблице 4;

M и $M + 1$ – два модуля, значение M равно количеству символов в наборе символов;

$\|_M$ – остаток после деления на M; если он равен нулю, то он заменяется на значение M;

$|_{M+1}$ – остаток после деления на $M + 1$; после этой операции остаток никогда не равняется нулю.

9.2 Позиция контрольного знака

Контрольный знак нужно поместить в крайний правый конец строки символов.

10 Метод расчета для гибридных систем

Существует только один базовый метод генерации и проверки символьных строк, защищенных гибридными системами. Это рекурсивный метод гибридной системы.

ПРЕДУПРЕЖДЕНИЕ – Вычислительные методы, аналогичные методу полиномов чистой системы, в этом случае НЕ дают того же результата и поэтому не используются.

10.1 Рекурсивный метод гибридных систем

10.1.1 Вычисление

В рекурсивном методе строка обрабатывается посимвольно слева направо.

Алгоритм генерирования контрольного знака α_1 может быть описан следующим образом. При индексе $j = 1 \ldots (n - 1)$, где n – количество символов в строке, включая контрольный знак, и определив $P_j = M$ для $j = 1$, получаем:

$$S_j := P_j |_{M+1} + \alpha_{n-j+1};$$

$$P_{j+1} := S_j \|_M \cdot 2,$$

где $\|_M$ – остаток от деления на M; если он равен нулю, то заменяется на значение M;

$|_{M+1}$ – остаток от деления на $M + 1$; остаток никогда не равняется нулю после этой операции;

α_{n-j+1} – значение символа.

Затем нужно выбрать α_1 таким, чтобы

$$P_n + \alpha_1 \equiv 1 \pmod{M}$$

или

$$\alpha_1 := (1 - P_n) \pmod{M}.$$

Алгоритм проверки контрольного знака α_1 можно описать следующим образом.

При индексе $j = 1 \ldots n$, где n – количество символов в строке, включая контрольный знак, и определив $P_j = 0$ для $j = 1$, получают

$$S_j := P_j |_{M+1} + \alpha_{n-j+1};$$

$$P_{j+1} := S_j \|_M \cdot 2.$$

Строка считается верной, если

$$S_n \equiv 1 \pmod{M}.$$

В качестве варианта процедуру генерации контрольного знака α_1 можно повторить. Строка считается верной, если сгенерированный контрольный знак соответствует существующему символу α_1.

10.1.2 Пример

Предположим, что в строку «0794» требуется добавить контрольный знак по системе ISO/IEC 7064, MOD 11,10 так, чтобы $M = 10$, $M + 1 = 11$ и $n = 5$ (т. е. 4 символа плюс 1 контрольный знак).

Выполняется расчет, как указано в таблице 10.

Таким образом, значение контрольного знака равно 5, а полностью защищенная строка – «07945». Следует отметить, что контрольный знак добавляется к исходной строке справа.

Таблица 10 – Пример рекурсивного метода гибридных систем

Шаг	Произведение, перенесенное вперед	+	Значение следующего знака	=	Промежуточная сумма	Скорректированная промежуточная сумма	x	2	=	Произведение	Скорректированное произведение, перенесенное вперед
j	P_j	+	α_{n-j+1}		S_j	$S_i\|\|_{10}$	x	2	=	P_{j+1}	$P_{j+1}\|_{11}$
1	10	+	0	=	10	10	x	2	=	20	9
2	9	+	7	=	16	6	x	2	=	12	1
3	1	+	9	=	10	10	x	2	=	20	9
4	9	+	4	=	13	3	x	2	=	6	6
5	6	+	контрольный знак (должен быть конгруэнтен 1 (mod 10))								

Чтобы выполнить проверку строки, шаги 1–5 в таблице 10 вычисляются, как показано, но контрольный знак 5 включается в расчет. Результат должен быть конгруэнтен 1 (mod 10).

Приложение А
(справочное)

Критерии выбора систем контрольных знаков для различных приложений

Критериями для выбора системы согласно таблице 11 являются:

a) набор символов защищаемой строки (столбец 2);

a) набор символов контрольных знаков (столбец 3): для всех систем, кроме ISO/IEC 7064, MOD 11-2 и 37-2, этот набор символов является таким же, как набор символов защищаемой строки. Для двух указанных систем необходимо использовать дополнительный контрольный знак либо не использовать строки, дающие значения контрольного знака для дополнительного контрольного знака;

b) количество контрольных знаков (столбец 4): приемлемость наличия двух контрольных знаков (с точки зрения стоимости или других ограничений) должна оцениваться с учетом такого преимущества, как повышенный уровень защиты, который обеспечивается системами с двумя контрольными знаками;

c) процент необнаруженных ошибок (столбец 5), т. е. процент ошибок каждого типа, которые, вероятно, останутся невыявленными. Такими типами ошибок являются:

1) единичное замещение – замещение одного символа другим символом;

2) единичная перестановка – перестановка отдельных символов, находящихся рядом (d = 1) или разделяемых одним символом (d = 2);

3) двойное замещение – две отдельные ошибки единичного замещения в той же строке;

4) циклический сдвиг – циклический сдвиг строк влево или вправо (уровень обнаружения указан только для циклических сдвигов на умеренные расстояния (d < 10));

5) прочее – все ошибки, не определенные выше;

6) остаточная ошибка (столбец 6).

Остаточная ошибка определяет типичный диапазон необнаруженных ошибок всех типов на 100 000 ошибок.

Более низкий показатель соответствует типичному наилучшему случаю благоприятных сочетаний типов ошибок. Более высокий показатель свидетельствует о неблагоприятных сочетаниях (например, при значении выше среднего возникновение ошибок не всегда обнаруживается). Эти цифры следует использовать в качестве руководства только при отсутствии надежной статистики. На практике могут встречаться значительные отклонения. Цифры в таблице 11 основываются на следующем типичном диапазоне показателей:

– единичное замещение	60 % – 85 %;
– единичная перестановка, d = 1	5 % – 15 %;
– единичная перестановка, d = 2	1 % – 2 %;
– двойное замещение	5 % – 15 %;
– циклический сдвиг	0 % – 5 %;
– прочие	1 % – 10 %.

Процент необнаруженных ошибок отражает результативность автономной работы систем контрольных знаков. Эффективным является сочетание систем контрольных знаков с другими проверками, такими как проверка совпадения результатов с заданным интервалом значений, проверка типа знака и длины строки, например проверка длины строки позволяет обнаружить все удаления и включения символов.

Таблица 11 – Сводный перечень критериев выбора систем

1	2	3	4	5						6
Система контрольных знаков ISO/IEC 7064, MOD	Набор символов защищаемой строки	Набор символов из контрольных знаков	Количество контрольных знаков	Процент необнаруженных ошибок						Остаточные ошибки на 100 000 ошибок
				Единичное замещение	Единичная перестановка		Двойное замещение	Циклический сдвиг	Прочее	
					$d = 1$	$d = 2$		$d < 10$		
11-2	Цифровой	Цифровой плюс «X» [1]	1	0,0	0,0	0,0	10,0	0,0	9,1	600–2400
11,10	Цифровой	Цифровой	1	0,0	2,2	9,3	11,0	0,0	10,0	760–3100
97-10	Цифровой	Цифровой	2	0,0	0,0	0,0	1,0	0,0	1,0	20–250
27,26	Буквенный	Буквенный	1	0,0	0,31	2,4	4,0	0,0	3,8	250–1100
661-26	Буквенный	Буквенный	2	0,0	0,0	0,0	0,1	0,0	0,15	6–30
37-2	Буквенно-цифровой	Буквенно-цифровой плюс «*» [2]	1	0,0	0,0	0,0	2,7	0,0	2,7	160–700
37,36	Буквенно-цифровой	Буквенно-цифровой	1	0,0	0,16	1,7	2,8	0,0	2,8	180–740
1271-36	Буквенно-цифровой	Буквенно-цифровой	2	0,0	0,0	0,0	0,04	0,0	0,08	3–15

[1] Дополнительного знака можно избежать, если не использовать строки, которые дают 10 в качестве значения контрольного знака.

[2] Дополнительного знака можно избежать, если не использовать строки, которые дают 36 в качестве значения контрольного знака.

Приложение В
(справочное)

Системы контрольных знаков для других алфавитов

В настоящем приложении показано, как можно разработать дополнительные системы для алфавитов, состоящих более чем из 26 букв.

В приведенном ниже примере применяется датский алфавит, насчитывающий 29 букв (от A до Z, Æ, Ø и Å).

Поскольку 29 является простым числом, а число 2 удовлетворяет условию, что наименьшим положительным числом α, для которого $2 \equiv 1 \pmod{29}$, является число 28 (= 29 − 1), то в данном случае может использоваться чистая система со значением модуля, равным 29, и основанием системы счисления, равным 2. Отличие от системы ISO будет состоять только в следующих элементах.

Обозначение: [Danish] MOD 29-2.

Таблица 4: дополнительные значения символов для буквенных систем:

Æ : 26

Ø : 27

Å : 28

Таблица 6: дополнительные весовые значения для MOD 29-2 из таблицы 12.

Таблица 12 – Весовые значения чистой системы для [Danish] MOD 29-2

Индекс позиции	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
[Danish] MOD 29-2	28	14	7	18	9	19	24	12	6	3	16	8	4	2	1

Библиография

[1] ISO 2108:1992 Information and documentation – International standard book numbering (ISBN)
(Информация и документация. Международный книжный стандартный номер (ISBN))

[2] ISO 2894:1980 Embossed credit cards – Specifications, numbering systems and registration procedure
(Тисненые кредитные карточки. Спецификации, системы нумерации и процедура регистрации)

[3] ISO 6166:2001 Securities and related financial instruments – International securities identification numbering system {ISIN}
(Ценные бумаги и относящиеся к ним финансовые инструменты. Международный идентификационный код ценной бумаги (ISIN))