УДК 621.391

М. В. Захарченко, В. Є. Басов, О. В. Кочетков, Д. В. Голев, А. С. Криль
Одеська національна академія зв'язку ім. О. С. Попова

ЗБІЛЬШЕННЯ ЕНТРОПІЇ КОДОВОГО СЛОВА У ДВІЙКОВОМУ КАНАЛІ ЗА ПОСТІЙНОЇ ТРИВАЛОСТІ

Інформація стає найважливішим національним ресурсом, відмінною рисою якого є те, що він не тільки не зменшується, а навпаки, – збільшується (передусім у разі обміну даними), якісно удосконалюється й разом з тим сприяє найраціональнішому використанню усіх інших видів інформаційних ресурсів. Під час передачі дуже важливо в кожному кодовому слові упаковувати більшу кількість інформації, тобто збільшувати ентропію. У роботі запропоновано алгоритм синтезу кодових слів у двійковому каналі з ентропією, що перевищує в десятки разів тривалість сигнальної конструкції.

Ключові слова: позиційні коди, ентропія, найквістовий елемент, інформаційна ємність, таймерна сигнальна конструкція, енергетична відстань

N. V. Zakharchenko, V. E. Basov, A. V. Kochetkov, D. V. Golev, A. S. Kril
O. S. Popov Odessa national academy of telecommunications

INCREASE IN AN ENTROPY OF A CODE WORD IN THE BINARY CHANNEL WITH CONSTANT DURATION

Transmission and perception of information are based on property of matter – reflection. Reflection is objective material process as a result of which system "A" interacting with system "B" reflects its image by change of the properties or acquires the new properties connected to closeness of system "B". Therefore, the content of reflection is defined by features of the displayed system "B", and the form of reflection – change of properties of the perceiving system "A".

Thus – information represents the internal content of process of reflection of one material objects in the form of change of properties of other objects.

Information transfer is best of all estimated by development of the communications industry which is characterized by four features.

The first feature is defined by specifics of the created product, namely – absence in case of information transfer of the material carriers of production.

The second feature of communication is tightly connected to the first, is defined by the fact that implementation process of communication services and their consuming is not time-shared. Taking into account this feature the end result of production activity of branch – the service, cannot be in reserve, for example, in a warehouse.

The third feature is that in the production process of the communications industry, information as an object of the labor, shall be subject only to spatial relocation, that is change of its location.

The fourth feature is that information transfer process always is double-sided, that is occurs between the sender and the receiver of information.

At the same time information becomes the major national resource which distinctive feature is that it not only does not decrease, and, on the contrary, – increases (generally in case

of a data interchange), is qualitatively enhanced and at the same time promotes the most rational use of all other types of information resources. In the course of spatial relocation it is very important to pack bigger amount of information in each code word, that is to increase an entropy.

In operation the synthesis algorithm of code words in the binary channel with the entropy exceeding duration of signal construction in tens of times is offered.

Key words: positional codes, entropy, Nyquist interval, information capacity, timer signal construction, energetic distance.

Вступ

Майже всі технічні засоби передачі інформації мають канали побічного витоку інформації [1]. Під витоком інформації розуміють несанкціоноване використання сторонніми особами, без відома власників, повідомлень, що передаються. Щоб ускладнити розуміння сенсу інформації у разі несанкціонованого використання повідомлення, запропоновано різні методи шифрування (спеціального кодування). Відмінність шифрування від надлишкового кодування полягає у тому, що під час шифрування черговий символ тексту, що передається, замінюється на інший символ цього тексту (цей "інший" символ визначається структурою тексту та параметрами відповідного кодового слова, яке називається "ключовим"). Варто зауважити, що під час шифрування кількість різних символів, що передаються, дорівнює кількості символів тексту, який передається, зі зміною імовірностей їх появи порівняно з початковим текстом [2].

Одним з недоліків такого методу шифрування є розмноження помилок під час дешифрування: помилка в одному символі шифрованого тексту призводить до великої кількості помилок під час дешифрування. Це явище часто спричиняє втрату великої кількості інформації.

Щоб зменшити розмноження помилок під час передачі шифрограми по каналу зв'язку, під час дешифрування, у роботі запропоновано алгоритм двократного передавання окремих символів за допомогою коректуючих таймерних сигналів [3].

Основні властивості таймерних сигнальних конструкцій

У разі використання масово двійкового позиційного кодування ентропія кодового слова (кодової конструкції) [4] визначається кількістю реалізацій ($N_{РП}$) кодових конструкцій:

$$H = \log_2 N_{\text{РП}}, \quad N_{\text{РП}} = a^n, \tag{1}$$

де a – основа коду (кількість різних значень інформаційного параметра); n – кількість елементів (посилок) у кодовому слові. Мінімальна тривалість кодового елемента (t_0) не може бути меншою від тривалості перехідного процесу [2]

$$t_{0\min} = 1/\Delta F, \tag{2}$$

де ΔF – смуга пропускання каналу. Отже, у разі позиційного кодування відстань між моментами модуляції кратна до найквістового елемента тривалістю t_0.

З вищесказаного випливає, що мінімальна енергетична відстань між кодовими конструкціями за позиційного кодування дорівнює енергії одного найквістового елемента тривалістю t_0. Зрозуміло, що збільшити кількість реалізацій на заданому інтервалі часу $T_{CK} = nt_0$ можна, тільки зменшивши енергетичну відстань між кодовими конструкціями [3]. Це завдання можна вирішити, використовуючи таймерні сигнальні конструкції.

На відміну від позиційного двійкового кодування, за якого інформація про кодове слово міститься в "n" найквістових елементах ("+" або "–"), у таймерних сигнальних конструкціях (ТСК) інформація про символ, що передається, міститься в "i" відрізках сигналів (t_{ci}), синтезованих на інтервалі $T_c = mt_0$, кожний з яких не менший від найквістового (t_0) [4]

$$t_{ci} = t_0 + z\Delta, \quad z \in (2;3...z_0) \text{ цілі}, \tag{3}$$

де Δ – частина елемента t_0 – ($\Delta = t_0/s, s \in (2;3;\mathbf{K}\, s_0)$ – цілі), яка забезпечує розпізнавальну здатність тривалостей окремих відрізків (t_{ci}) із заданою імовірністю помилки на виході каналу за відомої завадової обстановки [5]; m – кількість найквістових елементів, які беруть участь у формуванні цього ансамблю ТСК.

За сформульованих умов потужність реалізованого ансамблю N_{PT} на інтервалі $T_{ск} = mt_0$ визначається [5] так:

$$N_{\text{РТ}} = \frac{(ms - i(s-1))!}{i!(ms - is)!}. \qquad (4)$$

У табл. 1 наведено кількість реалізацій для позиційного кодування ($N_{\text{РП}}$) і синтезу ТСК ($N_{\text{РТ}}$) для m=(3÷10), за двох значень s (s_1=4; s_2=7) та двох i (i_1=3; i_2=4).

Таблиця 1

Кількість реалізацій за $m = (3 \div 10), s = 4;7, i = 3;4$

i	S	m	3	4	5	6	7	8	9	10
		$N_{\text{РП}}$	2^3=8	2^4=16	2^5=32	2^6=64	2^7=128	2^8=256	2^9=512	2^{10}=1024
3	4	$N_{\text{РТ}}$	1	35	165	455	969	1771	2925	4495
3	7	$N_{\text{РТ}}$	1	120	680	2024	4495	8436	14190	22100
4	4	$N_{\text{РТ}}$	0	1	70	495	1820	4845	10626	20475
4	7	$N_{\text{РТ}}$	0	1	330	3060	12650	35960	82251	163185

З табл. 1 випливає: 1) кількість реалізацій ТСК N_{PT} зростає зі збільшенням інтервалу реалізацій m; 2) в тому самому інтервалі синтезу ТСК ($m = const$) кількість реалізацій можна істотно збільшити, використовуючи ансамблі, які містять конструкції з різною кількістю відрізків "i".

У табл. 2 наведено імовірності помилкового приймання кодових слів у позиційному (ПК) та таймерному (ТК) кодуванні за близької рівності тривалостей.

Таблиця 2

Порівняння позиційного та таймерного кодування

ПК				ТСК, якщо $S = 7, (\Delta = 0{,}143t_0), i = 3$			
n	$N_{\text{пер}}$	$N_{\text{пом}}$	$P_{\text{пом}}$	n	$N_{\text{пер}}$	$N_{\text{пом}}$	$P_{\text{пом}}$
10	10^6	700	7×10^{-4}	9	10^6	104	$1{,}04\times10^{-4}$
20	10^6	770	$7{,}7\times10^{-4}$	17	10^6	1150	$11{,}5\times10^{-4}$
40	10^6	1500	15×10^{-3}	33	10^6	1620	$1{,}6\times10^{-3}$

У табл. 2 прийнято такі позначення: $N_{\text{пер}}$ – кількість переданих кодових слів; $N_{\text{пом}}$ – кількість помилково прийнятих кодових слів; n – довжина кодового слова найквістового елемента, $P_{\text{пом}}$ – імовірність помилкового приймання кодового слова.

З табл. 1, 2 випливає, що у двійковому каналі ентропія (H) кодових слів може перевищувати тривалість кодового слова – n. Такі можливості можна отримати, використовуючи ансамблі сигнальних конструкцій з різною кількістю інформаційних відрізків (t_{ci}) на інтервалі $T_{ск} = mt_0$,

якщо $m = const$. Отже, у двійковому каналі можна передавати на одному інтервалі Найквіста більше від одного біта інформації.

В табл. 3 наведено значення ентропії кодових слів (H) та інформаційної ємності найквістового елемента I_H за $m \in (3 \div 10); i \in (1 \div 10); s = 7$, що визначається формулою (5)

$$I_H = \frac{\log_2 N_{\text{PT}}}{m} = \frac{H}{m}. \quad (5)$$

Таблиця 3

Інформаційна ємність найквістового елемента

m	3		4		5		6	
i	H	I_H	H	I_H	H	I_H	H	I_H
1	3,907	1,302	4,459	1,115	4,858	0,972	5,17	0,862
2	5,17	1,723	6,907	1,727	7,983	1,597	8,765	1,461
3	0	0	6,907	1,727	9,409	1,882	10,983	1,831
4	–	–	0	0	8,366	1,673	11,579	1,93
5	–	–	–	–	0	0	9,629	1,605
6	–	–	–	–	–	–	0	0
7	–	–	–	–	–	–	–	–
8	–	–	–	–	–	–	–	–
9	–	–	–	–	–	–	–	–
10	–	–	–	–	–	–	–	–
$\sum N_{Pi}$	52		263		1293		6348	
$\sum H$	9,077		18,273		30,616		46,126	
$\sum I_H$		3,025		4,568		6,123		7,688
m	7		8		9		10	
i	H	I_H	H	I_H	H	I_H	H	I_H
1	5,426	0,775	5,644	0,706	5,833	0,648	6	0,6
2	9,379	1,34	9,886	1,236	10,316	1,146	10,691	1,069
3	12,134	1,733	13,042	1,63	13,793	1,533	14,432	1,443
4	13,627	1,947	15,134	1,892	16,328	1,814	17,316	1,732
5	13,505	1,929	16,005	2,001	17,857	1,984	19,328	1,933
6	10,745	1,535	15,242	1,905	18,175	2,019	20,359	2,036
7	0	0	11,745	1,468	16,827	1,87	20,175	2,018
8	–	–	0	0	12,652	1,406	18,287	1,829
9	–	–	–	–	0	0	13,482	1,348
10	–	–	–	–	–	–	0	0
$\sum N_{P_i}$	31198		153365		753835		3705165	
$\sum H$	64,816		86,698		111,781		140,07	
$\sum I_H$		9,259		10,838		12,42		14,008

Висновки

З табл. 3 випливає, що:

1) сумарні значення: потужності ансамблів $\sum N_{P_i}$ та сумарної інформаційної ємності $\sum I_H$ найквістового елемента збільшуються зі зростанням m;

2) за кожного i для $m \in 3 \div 10$ значення $m_{\max}$ (з максимальним значенням I_H) збільшується зі зростанням i. Наприклад:

$i=1$	$m_{\max}=3$	$i=3$	$m_{\max}=5$	$i=5$	$m_{\max}=8$
$i=2$	$m_{\max}=4$	$i=4$	$m_{\max}=7$	$i=6$	$m_{\max}=10$

3) сумарні значення $\sum H$ та $\sum I_H$ зростають зі збільшенням m (коефіцієнти зростання $K_1=\frac{\sum H_{m+1}}{H_m}$ та $K_2=\frac{\sum I_{H(m+1)}}{\sum I_{H\,m}}$ подано в табл. 4 для $m\in 3\div 10$);

Таблиця 4

Коефіцієнти зростання H та I_H

	3	4	5	6	7	8	9	10
K_1	–	2,013	1,675	1,507	1,405	1,338	1,289	1,253
K_2	–	1,51	1,34	1,256	1,204	1,171	1,146	1,128

4) підвищити інформаційну ємність найквістового елемента за постійного значення довжини кодового слова можливо тільки за рахунок створення ансамблів з різним значенням інформаційних відрізків, якщо $m=const$;

5) за кожного значення "m" у двійковому каналі сумарна інформаційна ємність $\sum H$ у декілька разів може перевищувати тривалість кодового слова m.

1. Методы прогнозирования защищенности ведомственных систем связи на основе концепции отводного канала / В. Г. Лихограй; под ред. А. И. Цопы, В. М. Шокало. – Харьков: КП "Городская типография", 2011. – 502 с. 2. Помехоустойчивость и эффективность систем передачи информации / А. Г. Зюко [и др.]; под ред. А. Г. Зюко. – М.: Радио и связь, 1985. – 232 с. 3. Захарченко М. В. Порівняння ансамблів кодових множин, синтезованих на основі декількох модулів, з ансамблями, реалізованими на основі таймерних сигнальних конструкцій / М. В. Захарченко, С. М. Горохов, О. В. Кочетков, В. В. Гордейчук, Е. Б. Шамшидін // Системи обробки інформації. – 2017. – № 1. – С. 18–21. 4. Захарченко Н. В. Таймерные сигнальные конструкции – как инструмент системы информационной безопасности / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский, Ю. С. Горохов // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2015. – № 1. – С. 256–260. 5. Захарченко Н. В. Сравнение позиционного и таймерного кодирования / Н. В. Захарченко, С. М. Горохов, А. В. Кочетков, В. В. Гордейчук // Збірник наукових праць [Військового інституту телекомунікацій та інформатизації]. – 2016. – Вип. 1. – С. 59–63.

References

1. Tsopa A. I., Shokalo V. M. (ed.), 2011, Methods for predicting the security of departmental communication systems based on the concept of a diversion channel, CE "City printing house", Kharkiv. 2. Zyuko A. G. (ed.), 1985, Interference immunity and efficiency of information transmission systems, Radio and communication, Moscow. 3. Zakharchenko N. V., Horokhov S. M., Kochetkov A. V., Gordeychuk V. V., Shamshidin E. B., 2017, Comparing ensemble code set synthesized based on several modules of the ensemble implemented on the basis timer signal constructions, Information processing systems, (147). 4. Zaharchenko M. V., Korchinsky V. V., Radzimovsky B. K., Gorohov Y. S., 2015, Timer signal design as a – tool of information security systems, Measuring and Computing Devices in Technological Processes, No. 1, P. 256–260. 5. Zakharchenko N. V., Horokhov S. M., Kochetkov A. V., Gordeychuk V. V., 2016, Compare the position coding and timing coding, Collection of scientific works "Military Institute of Telecommunications and Informatization", No. 1. – P. 59–63.