КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№3 (7), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.7.95102
УДК. 004.056

Захарченко Микола Васильович
Доктор технічних наук, професор, завідуючий кафедрою
Кафедра кібербезпеки та технічної захисти інформації
Одеська Національна Академія Зв'язку ім. О.С. Попова, Одеса
ORCID ID: 0000-0001-8946-7798
kaf.ibpd@onat.edu.ua

Гаджиев Матін Магсуд-огли
Доктор технічних наук, професор
Кафедра кібербезпеки та технічної захисти інформації
Одеська Національна Академія Зв'язку ім. О.С. Попова, Одеса
ORCID ID: 0000-0001-7280-3863
gadjievmm@ukr.net

Салманов Наріман Сулейман-огли
Кандидат технічних наук,
Керівник «Телеком» м. Сумгаїт, Азербайджан
ORCID ID: 0000-0002-0247-2517
nariman_s@box.az

Голев Денис Володимирович
Викладач
Кафедра кібербезпеки та технічної захисти інформації
Одеська Національна Академія Зв'язку ім. О.С. Попова, Одеса
ORCID ID: 0000-0002-2899-4436
denis_veteran@ukr.net

Швець Наталія Василівна
Старший викладач
Кафедра інформаційних технологій та кібербезпеки
Одеська національна академія харчових технологій, Одеса
ORCID ID: 0000-0002-6719-3842
shvetsnv0601@gmail.com

ІНФОРМАЦІЙНІ ПАРАМЕТРИ КОДОВИХ АНСАМБЛІВ, СИНТЕЗОВАНИХ НА ОСНОВІ ОДНОГО МОДУЛЯ

Анотація Переваги цифрових методів обробки, відображення, зберігання, передачі і прийому інформації забезпечують їм переважне використання в сучасних телекомунікаційних мережах зв'язку. У теперішній час для збільшення швидкості передачі інформації, збереження високої вірності прийому і забезпечення необхідної скритності передачі використовують різні методи цифрового перетворення і ефективні способи кодування. Зокрема, таймерні (часові) сигнальні конструкції, які в порівнянні з іншими методами кодування, наприклад, позиційного (порозрядне) кодування дозволяють знижувати витрати часу більш ніж в два рази. У роботі проведена оцінка інформаційних параметрів кодових ансамблів, синтезованих на постійній тривалості "m" найквістових елементів при використанні одного загального модуля. Визначено умови формування кодового ансамблю і розраховано число реалізацій кодових слів на відрізках декілька найквістових елементів. З метою ефективного використання каналу зв'язку запропонованого збільшення ентропії передаваємого ансамблю за рахунок використання кодових множин з різним числом інформаційних відрізків і при постійній довжині кодового

ISSN 2663 - 4023

слова. Суттєве збільшення ваги синтезуємого ансамблю забезпечила збільшення значення модуля $A_0 = 19$ в ціле число разів $K \in 8 \div 18$. В роботі розраховано максимальні значення модуля KA_0 при якому синтезується найбільша кількість кодових слів:
Якшо:
$KA_0 = 13;\ N_p = 8;$ $KA_0 = 14;\ N_p = 10$
$KA_0 = 15;\ N_p = 15;$ $KA_0 = 17\ N_p = 16$
$KA_0 = 18;\ N_p = 10;$ $KA_0 = 19\ N_p = 6$
$KA_0 = 20\ N_p = 1$
При вказаних значення KA_0 розраховано значення ентропії $H = 3.269$, що менше ентропії російського тексту $H = 4.35$.
Визначені і приведені у вигляді таблиці кодові слова, що задовольняють умовам рівняння якості. Проаналізовані методи та алгоритми достовірного прийому кодових слів при впливі перешкод у використовуваному каналі. Проведені дослідження і розрахунки показали, що використання таймерних сигнальних конструкцій, синтезованих на основі одного модуля дозволяють значно знизити значення ентропії для передачі російського тексту.

Ключові слова: інформація, найквістовий елемент, таймерні сигнальні конструкції, ентропія.

1.ВСТУП

Системою залишкових класів називається така непозиційна система числення, в якій будь-яке ціле додатне число подається у вигляді набору найменованих додатних залишків (вирахувань) від ділення цього числа на фіксовані цілі додатні числа P1, P2 … Pm, які називаються основами (модулями).

Позначимо $a_1 = |A|$ як найменший позитивний залишок від ділення цілого числа A на основу Pi. В такому випадку число A буде представлено декількома залишками a_i в залежності від кількості основ Pi Є P1; P2; P3 . . . Pm.

$$A = a_1; a_2; \dots a_m \quad (1)$$

Будь якому цілому числу A можна зіставити певний набір залишків $\{a_1; a_2; \dots a_m\}$, але зворотнє твердження справедливе лише в тому випадку – коли основи СЗК попарно прості. Якщо ця умова не виконується, то знайдуться такі набори $\{a_1; a_2; \dots a_m\}$, якими не можна зіставити жодного числа A.

Для довільної СЗК існує $M = [P_1;\ P_2; \dots P_m]^2$ різних наборів $\{a_1; a_2; \dots a_m\}$ кожному з яких можна зіставити множину цілих чисел виду

$$A = KM, \text{ де } K \in 0; 1; 2\ \vdots\ m.$$

В цьому випадку коли всі цілі A належать інтервалу, значення якого дорівнює M, то кожному набору $\{a_1; a_2; \dots a_m\}$ відповідає тільки одне число A. Число M називається загальною основою залишкових класів.

Визначення позиційних характеристик в системах СЗК.

ISSN 2663 - 4023

Розглянемо будь-яку позиційну систему числення з основними незалежними модулями $P_1, \dots, P_m$ множення яких відповідає числу M. Будемо вважати,

що $\left(\frac{M'}{P'_m}\right) < M \le M'$, в такому випадку будь-яке число в діапазоні $[0, M]$ можна представити в даній позиційній системі числення [1].

$$A = \sum a_i \prod_{j=1}^{i-1} P_j \quad (2)$$

В даній формулі P_j представляє один із модулів множини $N(M)$

$$N(M) = P_1 \times P_2 \times \dots \times P_m \quad (3)$$

Дані ансамблі характеризуються двома теоремами:

Теорема 1. Для будь-якого цілого числа $A = \{a_1; a_2; \dots a_m\}_M$, представленого в СЗК основами $P_1; \dots; P_m$, та для будь-якої пари основ P_i та P_j виконується умова:

$$\left|L_i - L_j\right|_{d_{ij}} = 0 \quad (4)$$

Де d_{ij} – найбільший загальний дільник для основ P_i і P_j.

Теорема 2. Якщо основами СЗК є взаємно-прості модулі (числа) то для будь-якого о дільника P_i дільник $d = 1$.

Слід зауважити, що добуток взаємно-простих модулів $P_i \in \frac{i}{m}$ характеризує потужність коду.

Для прикладу розглянемо структуру множини таймерних сигнальних конструкцій, синтезованих на інтервалі $m = T_c = 7t_0$ при $S = 5$ та $i = 3$.

Загальне число реалізацій N_p при заданих параметрах визначається [2,3]:

$$N_p = \frac{(mS - i(S-1))!}{i!(mS - iS)!} \quad (4)$$

Підставимо в вираз (4) вказані вище значення та одержимо $N_p = 1771$ кодових конструкцій. Із 1771-го кодового слова обираємо тільки ті, в яких суми 3-х відрізків кратні заданому модулю $P = 19$:

$\frac{1771}{19} = 93{,}2 \approx 94$ кодових слова.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

В таблиці 1 приведені 94 кодових слова, кожне з яких складається із 3-х відрізків, задовольняючих умові:

$$(A_1x_1 + A_2x_2 + A_3x_3) = 0 mod 19 \quad (5)$$

Визначимо вектор перешкоди який буде відповідати модулю 19, тобто спотворення не буде виявлено за умовою якості передачі (5) [4].

Припустимо, що передається вектор x1; x2; x3 дорівнював 0 по модулю 19, в цьому випадку спотворення тривалості окремих відрізків не будуть виявлені, якщо

$$A_1(x_1 + e_1) + A_2(x_2 + e_2) + A_3(x_3 + e_3) = (A_1x_1 + A_2x_2 + A_3x_3) + (A_1e_1 + A_2e_2 + A_3e_3)$$

ISSN 2663 - 4023

Таблиця 1. Кодові слова, що задовольняють рівність (2)

N_{kx} / λ_0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	5	6	5	7	5	6	7	8	5	6	7	8	9	8	6	6
2	10	11	11	12	15	12	16	13	12	16	13	17	14	15	13	20
3	16	18	21	20	22	23	21	22	26	24	25	23	24	27	28	25
KA_0 / λ_0	$8A_0$	$9A_0$	$10A_0$	$10A_0$	$11A_0$	$11A_0$	$11A_0$	$11A_0$	$12A_0$	$12A_0$	$12A_0$	$12A_0$	$12A_0$	$13A_0$	$13A_0$	$13A_0$
	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	7	8	9	10	11	5	5	6	7	7	8	9	10	11	12	5
2	17	24	18	15	19	13	20	17	14	21	18	15	19	16	20	10
3	26	27	15	26	24	31	28	29	30	27	28	29	27	28	26	35
KA_0 / λ_0	$13A_0$	$13A_0$	$13A_0$	$13A_0$	$13A_0$	$14A_0$	$14A_0$	$14A_0$	$14A_0$	$14A_0$	$14A_0$	$14A_0$	$14A_0$	$14A_0$	$14A_0$	$15A_0$
	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
1	5	5	6	6	7	8	8	9	10	10	11	12	13	15	5	6
2	17	24	14	21	18	15	22	19	16	23	20	17	21	22	21	18
3	32	29	33	30	31	32	29	30	31	28	29	30	28	27	33	34
KA_0 / λ_0	$15A_0$	$15A_0$	$15A_0$	$15A_0$	$15A_0$	$15A_0$	$15A_0$	$15A_0$	$15A_0$	$15A_0$	$15A_0$	$15A_0$	$15A_0$	$15A_0$	$16A_0$	$16A_0$
	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
1	6	7	7	8	9	9	10	11	11	12	13	14	16	5	6	7
2	25	15	22	19	16	23	20	17	24	21	18	22	23	25	22	26
3	31	35	32	33	34	31	32	33	30	31	32	30	29	34	35	33
KA_0 / λ_0	$16A_0$	$16A_0$	$16A_0$	$16A_0$	$16A_0$	$16A_0$	$16A_0$	$16A_0$	$16A_0$	$16A_0$	$16A_0$	$16A_0$	$16A_0$	$17A_0$	$17A_0$	$17A_0$
	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
1	8	9	9	10	11	12	12	13	14	14	15	17	19	5	8	10
2	23	20	27	24	21	18	25	22	19	26	23	24	25	29	27	28
3	34	35	32	33	34	35	32	33	34	31	32	31	30	35	35	34
KA_0 / λ_0	$17A_0$	$17A_0$	$17A_0$	$17A_0$	$17A_0$	$17A_0$	$17A_0$	$17A_0$	$17A_0$	$17A_0$	$17A_0$	$17A_0$	$17A_0$	$18A_0$	$18A_0$	$18A_0$
	81	82	83	84	85	86	87	88	89	90	91	92	93	94		
1	11	13	14	15	16	18	20	13	16	18	19	21	23	24		
2	25	26	23	27	24	25	26	30	28	29	26	27	28	29		
3	35	34	35	33	34	33	32	35	35	34	35	34	33	35		
KA_0	$18A_0$	$18A_0$	$18A_0$	$18A_0$	$18A_0$	$18A_0$	$18A_0$	$19A_0$	$19A_0$	$19A_0$	$19A_0$	$19A_0$	$19A_0$	$20A_0$		

Так як перша сума обчислення (3) задовольняє рівності 0 по mod19 за умови формування вихідного кодового слова, то вектор E (e_1; e_2; e_3) не буде виявлений в тих випадках, коли координати вектора помилки будуть так само рівні «0» по mod19.

З виразу (5) слідує, що вектор помилки з мінімальною вагою E буде не виявлено за умови, коли його координати становитимуть e_1=1; e_2=1; e_3=2 тоді 2 2*1+3*1+7*2 = 19, що відповідає модулю A_0=19, отже, спотворення не буде виявлено.

У таблиці 2 наведені частости використання окремих частот модулей KA_0 (N_p) ймовірності появи їх по відношенню до загальної кількості реалізацій (N_p=94) і значення складових ентропій (H) використання окремих значень KA_0.

ISSN 2663 - 4023

Таблиця 2. Таблиця частостей появ модуля $КА_0$

$КА_0$		8	9	10	11	12	13	14
N_p		1	1	2	4	5	8	10
Ймовірність появи	$P_i = \frac{N_p}{94}$	0,0106	0,0106	0,0212	0,0425	0,0531	0,0851	0,1063
Ентропія	$H = -\sum_{i=1}^{94} P_i \log_2 P_i$	0,0693	0,0697	0,1181	0,1938	0,2251	0,3025	0,3439

$КА_0$		15	16	17	18	19	20
N_p		15	15	16	10	6	1
Ймовірність появи	$P_i = \frac{N_p}{94}$	0,15957	0,15957	0,17021	0,10638	0,0638	0,01063
Ентропія	$H = -P_i \log_2 P_i$	0,42250	0,42250	0,43482	0,3439	0,2533	0,06973

Отримане в табл. 2 значення ентропії $H = 3{,}269$ менше величини ентропії для російського тексту ($H = 4{,}35$ [3,5]). Пояснюється це 2-ма причинами:
У табл. 2 числа N_p групуються, що зменшує ентропію за рахунок збільшення ентропії розглянутих подій. Більше половини кратності $КА_0$ перевищують значення Np > 10.

Відзначимо основні властивості ентропії [3]:
1). H = 0 тільки в тому випадку, коли всі ймовірності Pi при і є 1 ÷ 94 крім однієї дорівнюють нулю і ця єдина ймовірність дорівнює 1. Отже H = 0 тільки в разі повної визначеності оцінки стану системи, і в інших випадках H> 0. Це твердження випливає з того факту, що вірогідність подій «Pi» знаходяться в інтервалі між нулем і одиницею m є $0 \le P_i \le 1$, отже $-P_i \log_2 P_i \ge 0$.
2). При заданому числі станів системи «n», максимальне значення ентропії H можливо коли всі ймовірності P_i Є $P_1 = P_2 = P_3 \ldots P_n = \frac{1}{n}$
3). При обчисленні двох незалежних ансамблів

$$x = x_1; x_2; x_3 \ldots x_n$$
$$y = y_1; y_2; y_3 \ldots y_n$$

загальна ентропія системи [x y] дорівнює:

$$H(x,y) \le H(x) + H(y) \quad (6)$$

При цьому в сумі (6) знак рівності можливий лише в тому випадку, коли розглядаються незалежні події.

Оцінимо значення ентропії появи окремих значень $КА_0$ вважаючи що вони були рівновірогідні [3]

$$P1 = P2 = P3 \ldots Pm = \frac{1}{94}.$$
$$P1 = P2 = Pn - 1 = P94 = \frac{1}{94}.$$

ISSN 2663 - 4023

Для такого значення Рі величина ентропії Н системи складе:

$$H = -\sum_{i=1}^{94} P_i \log_2 P_i = -\log_2 P_i \,(P_1 + P_2 + P_3 \dots P_{94}) = -\log_2 P_i \left(\frac{1}{94} + \frac{1}{94} + \frac{1}{94} \dots \frac{1}{94}\right)$$
$$= -\log_2 1 + -\log_2 94 = 6{,}54.$$

Отримане значення ентропії більше значення 3,269 говорить про те, що при рівноймовірних подіях стан системи відповідає найбільшій невизначеності [3].

ВИСНОВКИ

Отримане в таблиці 2 значення ентропії (Н = 3,269) менше ентропії російського тексту за рахунок того, що реалізовані конструкції групуються по кратності модуля $КА_0$.

а) Найбільша вага синтезованих кодових слів при значеннях:

$KA_0 = 14;\ N_p = 10,\ KA_0 = 15;\ N_p = 15;$

$KA_0 = 17;\ N_p = 16,\ KA_0 = 18;\ N_p = 10;$

$KA_0 = 19;\ N_p = 6,\ KA_0 = 20;\ N_p = 1.$

б) Значення розрахованої ентропії при зміні модуля KA_0 менше ентропії російського тексту за рахунок групування кількості синтезованих кодових слів при окремих модулях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Зюко А.Г., Фалько А.Ц., Панфилов И.П, Банкет В.Л. и др. Помехоустойчивость и эффективность систем передачи информации. – М. Радиосвязь, 1985 г., 272с.

[2] Захарченко М.В. Системи передавння данних том 1. Заводостійке кодування, Одеса, Фенікс 2009 г., 448с.

[3] Цымбал В.П. Задачник по теории информации и кодированию. Издательство «Вища школа», Киев, – 1976 г., 275с.

[4] V. Korchinskyi, M. Hadzhiyev , P. Pozdniakov, V. Kildishev, V. Hordiychuk / Development of the procedure for forming non-stationary signal structures based on multicomponent LFM signals // Eastern-European Journal of Enterprise Technologies, 6/9 (96) 2018, Content, 29-38.

[5] V. Buriachok, M. Hadzhyiev, V. Sokolov, P. Skladannyi, L. Kuzmenko / Implementation of an index optimize technology for highly specialized terms based on the phonetic algorithm metaphone // Eastern-European Journal of Enterprise Technologies, 5/2 (101) 2019, Content, 64-72.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (7), 2020
ISSN 2663 - 4023

Zaharchenko Mikola
Doctor of Technical Sciences, Professor, Head of department
Department of Cybersecurity and Technical Information Protection
Odessa National Academy of Telecommunications O.S. Popova
ORCID ID: 0000-0001-8946-7798
kaf.ibpd@onat.edu.ua

Hadzhyiev Matin
Doctor of Technical Sciences, Professor
Department of Cybersecurity and Technical Information Protection
Odessa National Academy of Telecommunications O.S. Popova
ORCID ID: 0000-0001-7280-3863
gadjievmm@ukr.net

Salmanov Nariman
Ph.D
Head of department «Telekom Sumgait», Sumgait, Azerbaijan
ORCID ID: 0000-0002-0247-2517
nariman_s@box.az

Golev Denis
Lecturer
Department of Cybersecurity and Technical Information Protection
Odessa National Academy of Telecommunications O.S. Popova
ORCID ID: 0000-0002-2899-4436
denis_veteran@ukr.net

Shvets Natalya
Senior Lecturer
Department of Information Technologies and Cybersecurity
Odessa National Academy of Food Technologies
ORCID ID: 0000-0002-6719-3842
shvetsnv0601@gmail.com

INFORMATION PARAMETERS OF CODES THAT ARE SYNTHESIZED ON THE BASIS OF ONE MODULE

Annotation. The advantages of digital methods of processing, displaying, storing and transmitting information. Currently, various conversion methods and efficient coding methods are used to increase the speed of information transfer, maintain high accuracy and provide the required latent accuracy. In particular, timer (temporary) signal constructions, which, in comparison with other coding methods, for example, positional (bitwise) coding, can reduce costs by more than two times. In the work, the information parameters of the code ensembles synthesized at a constant duration "m" are evaluated. Determined the conditions for the formation of a code ensemble and calculate the number of code dictionary implementations on a segment of a nyquist elements.In order to use the communication channel efficiently, the proposed increase in the entropy of the transmitted ensemble is due to the use of code sets with different number of information segments and at a constant length of the code word. A significant increase in the weight of the synthesized ensemble ensured an increase in the value of the module $A_0 = 19$ integer times $K \in 8 \div 18$.The maximum values of the module KA_0 are calculated in which the greatest number of code words is synthesized:

At:
$KA_0 = 13;\ N_p = 8;$ $KA_0 = 14;\ N_p = 10$
$KA_0 = 15;\ N_p = 15;$ $KA_0 = 17\ N_p = 16$
$KA_0 = 18;\ N_p = 10;$ $KA_0 = 19\ N_p = 6$
$KA_0 = 20\ N_p = 1$
For these KA_0values, the entropy value is $H = 3.269$, which is less than the entropy of the Russian text $H = 4.35$. In accordance with code words that satisfy the conditions of the quality equation. The methods and algorithms of reliable reception of code words under the influence of interference in the channel used were analyzed.Studies and calculations have shown that the use of temporary signal structures synthesized on the basis of a one module can significantly reduce the value of entropy for the transmission of Russian text.

Keywords: information, nyquist element, temporary signal constructions, entropy.

REFERENCES

[1] A.G. Ziuko, A. Ts. Falko, I. P. Panfilov,V.L. Banket "Jamming immunity and efficiency of information transmission systems," Radyosviaz, Moscow, 272 p., 1985.

[2] M.V. Zakharchenko "Data transmission systems," Vol. 1, Odesa, Feniks, 2009, 448 p.

[3] V.P. Tsymbal "Task book on information theory and coding" Vyshcha Shkola, Kyiv, 1976, 275 p.

[4] V. Korchinskyi, M. Hadzhiyev, P. Pozdniakov, V. Kildishev, V. Hordiychuk / Development of the procedure for forming non-stationary signal structures based on multicomponent LFM signals // Eastern-European Journal of Enterprise Technologies, 6/9 (96) 2018, Content, pp. 29-38.

[5] V. Buriachok, M. Hadzhyiev, V. Sokolov, P. Skladannyi, L. Kuzmenko / Implementation of an index optimize technology for highly specialized terms based on the phonetic algorithm metaphone // Eastern-European Journal of Enterprise Technologies, 5/2 (101) 2019, Content, pp. 64-72.