УДК 004.056.52 DOI: 10.46972/2076-1546.2019.16.03

М. В. Захарченко, В. В. Гордійчук, О. Г. Данильчук

МОДУЛІ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ СКРИТНОСТІ

Аналіз засобів та принципів ведення радіоелектронної розвідки, а також технологій, які дозволяють отримати доступ до інформації, показує, що в умовах сьогодення зростає необхідність у підвищенні ефективності протидії їм. Саме тому актуальним завданням є пошук або синтез сигнальних конструкцій, що забезпечують необхідний рівень стійкості інформаційних повідомлень до можливості несанкціонованого доступу.

З цією метою в статті досліджено принципи формування сигналів на основі таймерного та позиційного кодування. Дані принципи значно відрізняються. За позиційного кодування тривалість окремих відрізків сигналу в кодовій конструкції може дорівнювати t_0, t_1 тощо. Отже, відстань між моментами модуляції кратна тривалості t_0, а кількість кодових слів становить 2^m. У ході використання таймерних сигнальних конструкцій кодове слово буде складатися з декількох інформаційних відрізків, які повинні відповідати умові $t_i = t_0 + z\Delta$, де $z \in 0;1;2;\ldots z_0$ – цілі числа. Тобто t_{ci} не може бути менше t_0, а $z\Delta$ містить інформацію про число.

У статті показано кількість реалізацій таймерних сигнальних конструкцій, потужність позиційного коду, розраховано ентропію з визначенням імовірності появи помилок за різних параметрів. Також розглянуто спосіб часового ущільнення за модулем A_0 та надано рекомендації щодо його використання для збільшення інформаційної скритності шляхом створення невизначеності в разі передачі під час шифрування.

Доведено, що використання модулів системи залишкових класів збільшить ефективність скритності інформації, що передається, за рахунок зміни ймовірності застосування окремих символів у шифрограмі, яка передається сигналом, побудованим на основі таймерних сигнальних конструкцій.

Ключові слова: *таймерні сигнальні конструкції; позиційні коди; ентропія; інформаційна скритність; елемент точності; несанкціонований доступ; інформаційна ємність.*

Постановка проблеми в загальному вигляді. З розвитком технологій радіоелектронної розвідки та несанкціонованого доступу (НСД) до інформації постійно зростає необхідність у підвищенні ефективності протидії їм. Можливими шляхами розв’язання цієї проблеми є покращення структурної та інформаційної скритності (криптостійкості) даних, що передаються.

Аналіз останніх досліджень і публікацій. НСД до інформації, що передається, передбачає виявлення і визначення структури сигналу, а також розкриття змісту повідомлення в разі його перехоплення [1], що зумовлює, у свою чергу, три види скритності сигнальних конструкцій: енергетичну, структурну й інформаційну. У зв'язку

з цим актуальним завданням є пошук і синтез таких сигнальних конструкцій, яким притаманні властивості скритності [5].

У роботі [2] описано суть таймерних сигнальних конструкцій (ТСК) та їх основні властивості. У [3] надано оцінку структурній та інформаційній скритності ТСК.

Повністю розкрито будову та властивості системи залишкових класів у [4].

Формулювання завдання дослідження. Метою статті є дослідження можливості підвищення стійкості до НСД до повідомлень, що передаються, за допомогою синтезу сигналів на основі ТСК та обробки символів відповідних шифрограм із застосуванням модулів системи залишкових класів.

Виклад основного матеріалу

1. Таймерні сигнальні конструкції

Принцип побудови ТСК полягає в такому: сигнальний алфавіт бінарних ТСК формується на інтервалі часу $\left(T_{ck} = mt_0\right)$ із мінімальною різницею довжин інформаційних відрізків величиною

$$\left|\tau_{ci} - \tau_{cj}\right| = \Delta, \ \left(\Delta = {t_0}/{S}\right).$$

Тоді на інтервалі кодового слова $T_{ck} = mt_0$ розташовано $n = mS$ відрізків Δ.

У разі позиційного кодування тривалості окремих відрізків сигналів передають двійкові цифри ("0" чи "1"), рівні тривалості найквістового елемента $t_0 = {1}/{\Delta F}$, де ΔF – смуга спектра, що пропускається (використовується). Залежно від статистичної структури переданих двійкових чисел тривалості окремих відрізків сигнали в кодовій конструкції можуть бути t_0, $2t_0$, $3t_0$ тощо. Отже, у разі позиційного кодування відстань між моментами модуляції T_M кратна тривалості t_0 $\left(T_M = kt_0; k \in \overline{1,n}\right)$, а кількість можливих кодових слів становить $N_k = 2^m$. Наприклад, якщо $m = 5$, то $N_k = 2^5 = 32$. За використання ТСК кодове слово складається з декількох інформаційних відрізків, які відповідають умові

$$t_i = t_0 + z\Delta, \tag{1}$$

де $z \in 0;1;2;\ldots z_0$ – цілі числа.

З рівняння (1) випливає, що τ_{ci} не може бути менше t_0, що забезпечує закінчення перехідного процесу, а другий доданок $z\Delta$ містить інформацію про число, яке передається. Це головна відмінність позиційного кодування (ПК) від таймерного: за ПК відстань між моментами модуляції кратна t_0, а за таймерного вона не менша найквістового елемента , але кратна Δ.

Остання особливість забезпечує істотне збільшення кількості реалізацій кодових слів на одному відрізку в разі таймерного кодування N_{PT} порівняно з позиційним $N_{PП}$ [2]:

$$N_p\left(при\ \ i=const\right)=C^{i}_{mS-i(S-1)}=\frac{\left[ms-i\left(s-1\right)\right]!}{i!\left(ms-is\right)!},\tag{2}$$

де $C^{i}_{m}=\frac{m!}{i!\left(m-i\right)!}$.

В (1)–(2) i позначає кількість відрізків у сигнальній кодовій конструкції. З даних виразів бачимо вплив окремих параметрів m, s, i на потужність N_{PT} реалізованої множини.

Для прикладу в табл. 1 наведено кількість реалізацій ТСК $\left(N_{PT}\right)$ на інтервалі $T_{ck}=mt_0s$ (в елементах Δ) і сигналів позиційного двійкового коду $N_{PП}=2^m$.

Таблиця 1

Кількість реалізацій ТСК і потужність позиційного коду $N_{PП}$ для деяких величин:

$i=3$, $T_c=mt_0s$ для $s\in 2\div 7$ та $N_{PП}=2^m$

m / s	$m=4$	$m=5$	$m=6$	$m=7$	$m=8$	$m=9$	$m=10$
	$N_{PП}=16$	$N_{PП}=32$	$N_{PП}=64$	$N_{PП}=128$	$N_{PП}=256$	$N_{PП}=512$	$N_{PП}=1024$
2	10	35	84	165	286	485	680
3	20	84	220	455	816	1330	2024
4	35	165	455	969	1771	2925	4495
5	56	286	816	1771	3276	5456	8436
6	84	455	1330	2925	5456	9139	14190
7	120	680	2024	4495	8436	14190	22900

З табл. 1 випливає: якщо $s=const$, то зі зростанням m кількість реалізацій набагато більша за $N_{PП}$; якщо $m=const$, то зі зростанням s кількість реалізацій N_P також збільшується.

У табл. 2 наведено значення величини інформації в кодових словах – ентропії $\left(H\right)$ у разі $s\in 2;3;4;5;6;7$ на інтервалі $T_{ck}\in\left(4\div 10\right)t_0$ при $i=3$, а в табл. 3 – інформаційну ємність $\left(J_H\right)$ найквістового елемента, що визначаються за такими формулами [3]:

$$\left.\begin{aligned} H&=log_2\,N_p\\ J_H&=\frac{H}{m}\end{aligned}\right\}.\tag{3}$$

Таблиця 2

Ентропія H кодових слів, якщо $m\in\left(4\div 10\right)t_0$, $s\in 2\div 7$, $i=3$

m / s	4	5	6	7	8	9	10
2	3,3	5,1	6,4	7,3	8,1	8,8	9,4
3	4,3	6,4	7,8	8,8	9,6	10,3	11
4	5,1	7,3	8,8	9,9	10,8	11,5	12,1
5	5,8	8,1	9,6	10,8	11,6	12,4	13
6	6,4	8,8	10,3	11,5	12,4	13,1	13,8
7	6,9	9,4	11	12,1	13	13,8	14,4

Таблиця 3

Інформаційна ємність J_H, якщо $m \in (4 \div 10)t_0$, $s \in 2 \div 7$, $i = 3$

s \ m	4	5	6	7	8	9	10
2	0,830482	1,065386	1,025857	1,052332	1,019984	0,98108	0,94039
3	1,080482	1,296893	1,278463	1,261389	1,209053	1,153023	1,098299
4	1,282321	1,47162	1,473264	1,417193	1,348794	1,279358	1,213411
5	1,451839	1,631974	1,612071	1,541478	1,459715	1,379292	1,304234
6	1,598079	1,765945	1,729535	1,644889	1,551703	1,46198	1,379259
7	1,726723	1,881878	1,830499	1,733444	1,630293	1,53251	1,443176
8	1,841581	1,984071	1,919037	1,810882	1,698896	1,594003	1,498855
9	1,94534	2,075442	1,997877	1,879689	1,759769	1,648516	1,54818
10	2,039968	2,15807	2,068938	1,941596	1,814478	1,697472	1,592453

З табл. 2–3 випливає:

зі зростанням m для всіх значень s ентропія H зростає;

якщо $s = const$, то зростає m, а інформаційна ємність найквістового елемента максимальна за $m = 5$;

якщо $m = const$, то зростає s, збільшується величина J_H (імовірність помилок також зростає за рахунок зменшення Δ).

Необхідно зазначити, що інформаційна ємність одного найквістового елемента зростає до значення $m = 5$, а якщо $m > 5$, то вона зменшується (табл. 3). Отже, ефективна швидкість передачі, тобто кількість інформації, що передається, на інтервалі $T_{ck}(4 \div 6)t_0$ збільшується, а на $T_{ck}(6 \div 10)t_0$ зменшується.

На рис. 1 показано залежності інтервалу реалізації (m) для заданої кількості N_{PT} у разі збільшення s.

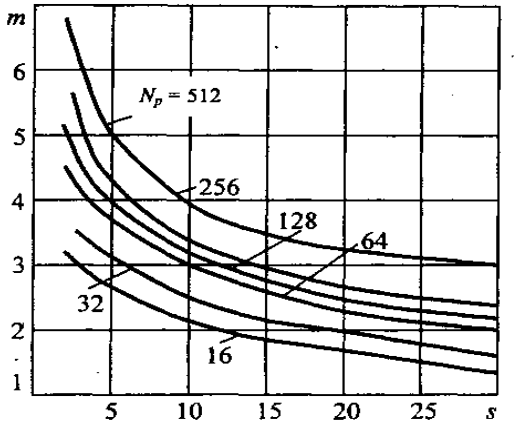

Рис. 1. Залежності тривалості сигнальної конструкції в разі заданої потужності кодової множини та параметра s

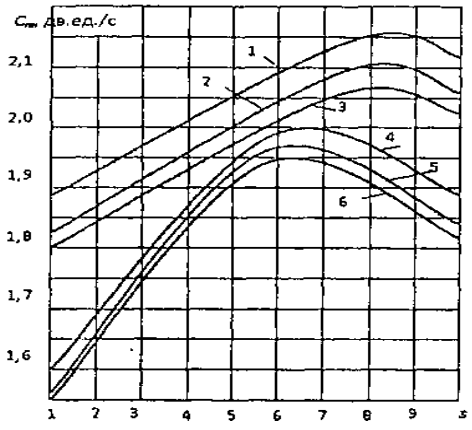

Рис. 2. Залежності пропускної здатності каналу $C_i = f(S)$ за $h = const$, $m = const$

Враховуючи, що кількість інформації, яка надходить до одержувача, менша тієї, що передається, на величину H_n (втрат) [2], то

$$H_n = -\left[P_{np} \log_2 P_{np} + \left[\left(1 - P_{np}\right) \log_2 \frac{1 - P_{np}}{N_p} \right] \right], \tag{4}$$

де P_{np} – імовірність правильного прийому.

Отже, швидкість передачі інформації на 1 елемент дорівнює

$$C = \frac{1}{m} \left[\log_2 N_p - H_n \right] \text{біт/с.} \tag{5}$$

На рис. 2 наведено залежності швидкості передачі $c = f(s)$ для двох значень h: залежності 1, 2, 3 для $h_1 = 7{,}5$ та $m = 8, 6, 5$ відповідно; залежності 4, 5, 6 для $h_2 = 5{,}5$ і для тих самих значень m.

З рис. 2 випливає, що для кожного значення h існує величина зони $\Delta(s)$, за якої C_m буде максимальною: зростаюча частина зазначених залежностей характеризується великим впливом збільшення кількості реалізацій (5), а спадна – значним впливом втрат H_n (2).

2. Часове ущільнення за $(mod\ A_0)$

З метою створення умов оцінювання якості передачі в ТСК, що формуються, значущі моменти модуляції розташовані на місцях, які відповідають певним співвідношенням [3]:

$$A_1 x_1 + A_2 x_2 + \ldots + A_n x_n \equiv 0 (mod\ A_0), \tag{6}$$

де x_n – тривалості окремих інформаційних відрізків у межах сигнальних конструкцій;

A_i – цілі числа, що визначають кодову відстань (у Δ) дозволених сигнальних конструкцій.

Окрім цього, за використану множину можуть синтезуватися кодові конструкції як з однаковою кількістю інформаційних відрізків i, так і з різною. Для створення умов конфіденційності модулі порівняння доцільно змінювати, що забезпечує збільшення інформаційної скритності.

Розглянемо багатоканальну систему з модульним поділом.

Припустимо, що є чотири різні модулі: $A_{01} = 11$, $A_{02} = 13$, $A_{03} = 17$, $A_{04} = 19$. Нехай інтервал реалізації $T_{ck} = 7t_0$ за $s = 7$, $i = 3$.

Згідно з виразом (2) кількість реалізацій з трьома відрізками буде $N_p = 4495$ [2]. Із цієї множини відповідати умовам (6) за різних A_{0i} будуть тільки $N_{PT}(A_{0i})$ [3]:

$$N_p'(A_0(i)) = N_{PT} \Big/ A_{0i}. \tag{7}$$

Тоді кількість реалізацій, які задовольняють умову (6), становить: $N_p'(11) = 4495/11 \approx 409$, $N_p'(13) = 4495/13 \approx 345$, $N_p'(17) = 4495/17 \approx 265$, $N_p'(19) = 4495/19 \approx 236$.

З огляду на те, що в зазначених $N_p'(A_0)$ є однакові сигнальні конструкції, за різних суміжних A_0 маємо:

$$N_p(11)\bigcap N_p(13)=36,\ N_p(11)\bigcap N_p(17)=20,$$
$$N_p(11)\bigcap N_p(19)=28,\ N_p(13)\bigcap N_p(17)=28,$$
$$N_p(13)\bigcap N_p(19)=13,\ N_p(\ )17\bigcap N_p(19)=12),$$

їх необхідно виключити в тій множинні $N_p(A_0)$, у якій міститься більше число N_P.

Унаслідок виключень отримаємо:

$$N_p(11)/\bigcap=409-(36+20+28)=325,$$
$$N_p(13)/\bigcap=345-(28+13)=301,$$
$$N_p(17)/\bigcap=265-12=253.$$

Будемо вважати, що загальна кількість переданих символів становить 60: 32 літери російської мови; 10 цифр; 4 символи арифметичних дій; 2 символи суми і добутку; 2 символи включення і виключення; 10 грецьких символів.

60 символів, що підлягають передачі, кодуються в кожній групі за різними модулями. Оскільки їх чотири, то в ході хаотичного вибору синтезується одна з комбінацій символу при цьому модулі.

З метою створення більшої невизначеності для сторонніх осіб символи краще передавати з різними значеннями модулів A_0. Наприклад, символи на позначення: голосних звуків – з $mod\,11$, приголосних – з $mod\,13$, арифметичних дій – з $mod\,17$, грецьких літер – з $mod\,19$ тощо.

Для збільшення невизначеності передачі під час шифрування для кожного переданого символу можна використовувати заміну його на символ, зміщений в алфавіті на z номерів, або застосувати спосіб змішування. Величина z може змінюватися відповідно до модуля порівняння: змінюючи його, можна одночасно змінювати і кількість інформаційних відрізків "i" у кодових словах, що формуються на передачу.

Висновки. У статті розглянуто особливості формування ТСК та їх можливості щодо підвищення скритності інформації, якої досягають за рахунок складності детермінації (дешифрування) сигналу, оскільки його структура є принципово новою порівняно з відомими: зміщено значущі моменти модуляції (на відміну від позиційних сигналів); інформацію поелементно закладено у відрізках, не кратних найквістовому елементу тощо.

З тією ж метою розглянуто властивості системи залишкових класів, за допомогою якої можна задавати ряд невизначеностей щодо послідовності кодованих символів: символи, що підлягають передачі, необхідно надсилати з різними значеннями модулів A_0; для кожного переданого символу слід використовувати заміну його на символ, зміщений в алфавіті на z номерів, або використовувати їх змішування.

Отже, доведено, що використання модулів системи залишкових класів збільшить ефективність скритності інформації, що передається, за рахунок зміни ймовірності застосування окремих символів у шифрограмі, яка передається сигналом, побудованим на основі ТСК.

СПИСОК ЛІТЕРАТУРИ

1. Куприянов А. И., Сахаров А. В. Теоретические основы радиоэлектронной борьбы. Москва : Вузовская книга, 2007. 356 с.
2. Захарченко М. В. Системи передавання даних. Т. 1. Завадостійке кодування. Одеса : Фенікс, 2009. 477 с.
3. Таймерные сигнальные конструкции как инструмент системы информационной безопасности / М. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский, Ю. С. Горохов // Вимірювальна та обчислювальна техніка в технологічних процесах. 2015. № 1. С. 256–259.
4. Обработка информации в системе остаточных классов (СОК) : учеб. пособ. / Н. И. Червяков, П. А. Ляхов, Л. Б. Копыткова, А. В. Гладков. Ставрополь : Изд-во СКФУ, 2016. 225 с.
5. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. Киев : Юниор, 2003. 504 с.

Подано 20.12.2018

Н. В. Захарченко, В. В. Гордейчук, А. Г. Данильчук

МОДУЛИ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ КАК ИНСТРУМЕНТ ИНФОРМАЦИОННОЙ СКРЫТНОСТИ

Анализ средств и принципов ведения радиоэлектронной разведки, а также технологий, которые позволяют получить доступ к информации, показывает, что в современных условиях возрастает необходимость в повышении эффективности противодействия им. Именно поэтому актуальной задачей является поиск или синтез сигнальных конструкций, обеспечивающих необходимый уровень стойкости информационных сообщений к возможности несанкционированного доступа.

С этой целью в статье исследованы принципы формирования сигналов на основе таймерного и позиционного кодирования. Данные принципы сильно отличаются. При позиционном кодировании длина отдельных сегментов сигнала в структуре кода может быть равна t_0, t_1 *и т. д. Таким образом, расстояние между моментами модуляции кратно длине* t_0 *и точному количеству кодовых слов* 2^m. *При использовании таймерных сигнальных конструкций кодовое слово будет состоять из нескольких информационных разделов, которые должны соответствовать условию* $t_i = t_0 + z\Delta$, *где* $z \in 0;1;2;\dots z_0$ – *целые числа. Следовательно,* t_{ci} *не может быть меньше* t_0, *а* $z\Delta$ *содержит информацию о числе.*

В статье показаны количество реализаций таймерных сигнальных конструкций и мощность кода позиции, рассчитана энтропия, указывающая вероятность ошибок в различных параметрах. Также рассмотрен метод консолидации времени по модулю A_0 *и даны рекомендации по его использованию для повышения скрытности информации путем генерирования неопределенности при передаче во время шифрования.*

Кроме того, доказано, что использование модулей системы остаточных классов увеличит эффективность скрытности информации, передаваемой сигналом, построенным на основе таймерных сигнальных конструкций.

Ключевые слова: *таймерные сигнальные конструкции; позиционные коды; энтропия; информационная скрытность; элемент точности; несанкционированный доступ; информационная емкость.*

M. V. Zaharchenko, V. V. Hordiichuk, O. G. Danylchuk

MODULES OF THE RESIDUAL CLASSES' SYSTEM AS AN INFORMATION ACCURACY TOOL

An analysis of the means and principles of electronic intelligence, as well as technologies, that allow access to information, shows that in modern conditions, the need for increasing the effectiveness of countering them is growing. That is why the urgent task is the search or synthesis of signal structures that provide the necessary level of resistance of information messages to the possibility of unauthorized access.

To this end, the article explores the principles of signal generation based on timer and position coding. These principles are very different. In positional coding, the length of individual signal segments in the code structure can be equal t_0, t_1 *and so on. Thus, the distance between the moments of modulation is a multiple of the length* t_0 *and the exact number of code words* 2^m. *When using timer signal constructions, the code word will consist of several information sections that must correspond to the condition* $t_i = t_0 + z\Delta$, *where* $z \in 0;1;2;...z_0$ *are integers. Therefore,* t_{ci} *cannot be less* t_0, *but* $z\Delta$ *contains information about the number.*

The article shows the number of implementations of timer signal structures and power of the position code, entropy calculated indicating the probability of errors in various parameters. Also considered is a modular time consolidation method and recommendations are given for its use to increase the secrecy of information by generating uncertainty during transmission during encryption.

In addition, it is proved that the use of modules of the system of residual classes will increase the efficiency of secrecy of information transmitted by a signal constructed on the basis of timer signal structures.

Keywords: *timer constructions; position codes; entropy; precision element; information secrecy; preciseness element; information capacity.*