УДК 004.056.52

В.В. Гордейчук
Институт Военно-Морских Сил Национального университета «Одесская морская академия», Украина

УВЕЛИЧЕНИЕ СКРЫТНОСТИ ПЕРЕДАВАЕМЫХ СООБЩЕНИЙ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

В работе рассмотрен метод шифрования передаваемого текста с использованием разрешенных кодовых множеств с различными модулями уравнения качества и дополнительным изменением номеров кодовых символов в исходной таблице.

Ключевые слова: *информационная безопасность, информационная скрытность, передача информации, таймерные сигнальные конструкции, система остаточных классов*

Анализ последних исследований. Постановка проблемы. Постановка задачи исследования.

В теории электрической связи различают два вида источников сообщений и сигналов: непрерывные и дискретные [1].

Примерами непрерывного сообщения может быть датчик температуры, атмосферного давления или величина напряжений на выходе микрофона.

Легко показать, что число различных значений напряжений на выходе микрофона зависят от допустимой погрешности измерительного прибора: чем меньше погрешность измерения прибора, тем больше различных значений он показывает. Из сказанного следует сделать вывод, что непрерывными называются источники и сигналы, характеризующиеся бесконечным значением своего состояния на конечном интервале времени (с увеличением различительной способности измерительного прибора).

Дискретными источниками и сообщениями называются такие устройства или сообщения, которые на бесконечном интервале времени характеризуются конечным числом своих состояний. Например, в книге «Война и мир» используется конечное число букв (32), в успеваемости студентов используются четыре цифры и т.д.

Конечное множество μ различных символов образует алфавит источников (число различных букв, символов) сообщений.

С момента использования первого аппарата П.Л. Шилинга (1786-1837) используются [2] двоичные коды (для двоичных каналов), в которых для передачи используется минимальный по длительности сигнал t_0, определяемый полосой пропускания канала ΔF с максимальным количеством элементов n_m [2].

$$t_0 = 1/\Delta F$$
$$n_m = E^+[\log_2 N_p], \quad (1)$$

где E^+ - символ целого ближайшего большего числа; N_p - число передаваемых различных символов.

Для упрощения системы синхронизации и фазирования [3] кодовые слова выбираются с одинаковым числом элементов $n = n_m$ с таким условием чтобы

$$2^{n_m} \geq N_p \quad (2)$$

Таким образом, все номера множества N_p записываются в двоичном виде с добавлением слева от последней единицы дополнительных нолей (до пяти двоичных единиц при $N_P = 32$), которые представляют пятиэлементный код [3].

Для обеспечения возможности структуре кодового слова реагировать на искажения отдельных элементов к информационным 5-ти элементам (m) добавляются проверочные r-элементов [4]

$$n = m + r \tag{3}$$

При этом число избыточных элементов r определяются из неравенства Варшамова-Гильберта [4]

$$2^{n-m} = 2^r \geq \sum_{i=0}^{d_0-2} C_{n-1}^i \tag{4}$$

Из (4) следует, что число дополнительных элементов (r) зависит не только от элементности простого кода (m), а и от искомого кодового расстояния d_0.

Из таблицы 1 можно проследить влияние значения величины кодового расстояния (d_0) на число избыточных элементов при позиционном кодировании.

Таблица 1

Зависимость числа избыточных элементов от величины кодового расстояния (d_0) при позиционном кодировании

m \ d_0	Число проверочных элементов r															
	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	3	3	3	4	4	4	4	4	4	4	5	5	5	5	5	5
4	5	5	6	6	7	7	7	7	8	8	8	8	8	8	9	9
5	7	8	8	9	9	10	10	10	11	11	11	12	12	12	12	12
6	9	10	11	11	12	12	13	13	14	14	14	15	15	15	15	16
7	11	12	13	14	15	15	16	16	17	17	17	18	18	18	19	19

Вводимые в кодовые слова избыточные элементы r позволяют только обнаруживать или обнаруживать и исправлять ошибки.

Как показал М. Плоткин [5] между кратностью исправляемой ошибки (исправляющей способностью кода) существует функциональная связь

$$d_0 = \frac{n(m-1)m^{k-1}}{m^k - 1}. \tag{5}$$

При этом исправляемая кратность ($z_{\max}$) искаженных символов

$$z_{\max} = \begin{cases} d_0 - 1/2, & d - нечетное \\ d_0 - 2, & d - четное \end{cases} \tag{6}$$

Исходя из таблицы 1, к недостаткам позиционного кодирования следует отнести:

- большая доля избыточных элементов r (при некоторых значениях d - значение $r > m$);
- минимальная длительность одного элемента для передачи цифр «0» или «1» равна длительности найквистового элемента $t_0 = \frac{1}{\Delta F}$, и меньше быть не может;

- расстояние между моментами модуляции в двоичном канале кратно элементу Найквиста;

- минимальное энергетическое расстояние между кодовыми словами равно энергии найквистового элемента. Именно это минимальное энергетическое расстояние исключает возможность реализовать большее количество кодовых слов в сравнении $N_p = 2^5 = 32$.

Таким образом, для получения большего числа реализаций необходимо уменьшить минимальное энергетическое расстояние между кодовыми словами на заданном интервале $T_{ek} = mt_0$.

Изложение основного материала

1. Основные свойства таймерных кодов

В отличие от позиционного кодирования, при котором информация о передаваемом символе содержится в знаке [(+) или (-)] отдельных найквистовых элементов кодовой комбинации, в таймерных кодах, информация о передаваемом символе содержится в длительностях отдельных (i) отрезков сигнала (T_{ck}) входящих в данное кодовое слово и удовлетворяющих условию [2].

$$T_{ck} = t_0 + z\Delta; \quad \Delta = \frac{t_0}{s}. \qquad (7)$$

где $z \in 2 \div z_0$; - целые, Δ - минимальное значение длинны отрезков T_{ck}, которое можно оценить при данной помеховой обстановке в канале (с учетом требуемой вероятности ошибок различной кратности) [6].

Именно элемент Δ позволяет увеличить число реализаций N_p на заданном интервале, имеющих меньшее энергетическое расстояние по сравнению с энергией найквистового элемента.

Количество реализаций в таймерах сигналах определяется выражением [4]:

$$N_p = \frac{[ms - i(s-1)]!}{i!(ms - is)!} \qquad (8)$$

В таблице 2 приведено числа реализаций на интервале $m \in 4 \div 10$ при $i_1 = 3$; $i_2 = 4$ для $s \in 3;5;7$, которое вычислено согласно (8).

Таблица 2

Число реализаций ТСК N_p при i =3,4; m =4÷10; s =3,5,7

i	s \ m	**4**	**5**	**6**	**7**	**8**	**9**	**10**
3	**3**	20	84	220	455	816	1330	2024
	5	56	286	816	1771	3276	5456	8436
	7	120	680	2024	4495	8436	14190	22100
4	**3**	1	35	210	715	1820	3876	7315
	5	1	126	1001	3876	10626	23751	46376
	7	1	330	3060	12650	35960	82251	183185
N_{pn}		16	32	64	128	256	512	1024

Из Таблицы 2 следует: 1) Что число N_P растет с увеличением m при $i = const$, 2) с увеличением i при $s = const$; $m = const$; N_P также увеличивается.

Подчеркнем, что числа в *Таблице 2* показывают, на сколько больше различных сигнальных конструкций состоящих из i -отрезков можно получить по сравнению с позиционным кодированием N_{pn}. В количества N_P входят кодовые множества с различным кодовым расстоянием.

Отметим основные свойства таймерных кодов:

1) при $i > m$ $N_p = 0$;

2) при $i = m$ $N_p = 1$ и этой сигнальной конструкции соответствует знако-переменный сигнал;

3) составляя ансамбли кодовых множеств необходимо использовать различные подмножества, в которых соблюдены условия:

а) одинаковый интервал реализаций (m);

б) одинаковое значение Δ (s);

в) различные значения i;

2. Модульное сравнение оценки качества передачи

Для возможности оценки правильности приема кодового слова можно из общего числа реализаций выбрать только те кодовые слова, у которых длительности τ_{ci} отдельных отрезков, входящих в данное кодовое слово, удовлетворяли условию (для $i = 3$) [2].

$$A_1\tau_{c1} + A_2\tau_{c2} + A_3\tau_{c3} = 0(\mathrm{mod}A_0) \qquad (9)$$

где: $A_1 \neq A_2 \neq A_3$ - целые простые числа.

Предположим, что мы хотим реализовать 4 канала передачи, которые отличаются по модулям A_{0i}: $A_{01} = 11$; $A_{02} = 13$; $A_{03} = 17$; $A_{04} = 19$.

Исходя из условия (9) при указанных модулях $A_0 \in A_{01} \div A_{04}$ и общего числа реализаций при $s = 7$; $m = 7$; $i = 3$; $N_{PT} = 4495$ [таблица 2] число реализаций, удовлетворяющих ему, будет равно:

$$N_{P1}(A_{01} = 11) = \frac{4495}{11} \approx 408; \qquad N_{P2}(A_{02} = 13) = \frac{4495}{13} \approx 345;$$

$$N_{P3}(A_{03} = 17) = \frac{4495}{17} \approx 264; \qquad N_{P4}(A_{04} = 19) = \frac{4495}{19} \approx 236.$$

Анализ множеств $N_{P1} \div N_{P4}$ показывает, что в множествах с различными модулями имеются одинаковые (повторяемые) кодовые слова.

Ясно, что для однозначности кодирования и декодирования их в одной из пары множеств необходимо исключить.

В Таблице 3 приведены числа повторяемых кодовых слов при различных модулях A_{0i}.

Таблица 3

Число повторяемых комбинаций при различных модулях A_{0i}.

A_{0i}	**11**	**13**	**17**	**19**	Σ
11	0	5+31	20	28	84
13		0	28	2+11	41
17			0	12	12
19				0	
					Σ 137
N_Σ	$\frac{4495}{11} \approx 408$	$\frac{4495}{13} \approx 345$	$\frac{4495}{17} \approx 264$	$\frac{4495}{19} \approx 236$	
$N_{исп}$	$408-84=324$	$345-41=301$	$264-12=252$		

После исключения останутся только неповторяемые кодовые слова (N_H)

$$N_H(A_{01}=11)=408; \qquad N_H(A_{02}=13)=345;$$
$$N_H(A_{03}=17)=264; \qquad N_H(A_{04}=19)=236.$$

Для удобства пользователя, в каждом множестве целесообразно оставить 60 кодовых слов: 32 кодовых символа для передачи 32 букв; 10 - для передачи цифр, и 18 для передачи других символов: (4 - арифметические операции, 2 - знаки включения-исключения, 10 знаков греческого алфавита).

В каждом множестве из 60 кодовых слов, удовлетворяющих условию (9) закодированы одни и те же символы (буквы, цифры и т.д.).

По согласованию с принимающей стороной порядок присвоения можно менять, что увеличивает трудность чтения шифрограммы.

Проведем количественную оценку множеств с различными кодовыми расстояниями.

С целью уменьшения расчетов, возьмем интервал реализаций $m=4$, $s=4$, $i=3$. Согласно выражению (1) $N_{P2}=35$. Построим матрицу 35×35 (причем она симметрична относительно главной диагонали, на которой нули) кодовых слов и определим какое количество кодовых слов имеют одинаковое кодовое расстояние. В таблице 4 приведены частоты появления кодовых слов с одинаковым значением d (под кодовым расстоянием понимается суммарные величины отличий (в Δ) каждой пары соответствующих отрезков сравниваемых кодовых слов).

Таблица 4

Частоты появления кодовых слов с одинаковым d

d	1	2	3	4	5	6	7	8	9	10	11	12
$\sum=595$	61	116	102	113	81	51	33	19	11	5	2	1

Из таблицы 4 следует, что для выбора 60 разрешенных кодовых слов с максимальным d можно взять множество с $d_0=5$

Заключение. Направление дальнейших исследований

Для увеличения времени прочтения шифрограммы кодовые слова одних и тех же символов можно передавать с различными модулями A_{0i} с дополнительным изменением их номеров в исходной таблице. Этот способ повышения криптостойкости и станет предметом дальнейших исследований по повышению информационной безопасности передаваемых сообщений в целом.

Список использованной литературы

1. Зюко А.Г., Фалько А.Н., Банкет В.Л. — Помехоустойчивость и эффективность систем передачи информации: Радио и связь, 1985 -304с.

2. Системи передавання данних. Том1. Ефективність блокового кодування. Захарченко М В., Кільдишев В.Й., Мартинова та інші, 2014, ОНАЗ ім. О.С.Попова - 487с.

3. Цымбал В.П. Задачник по теории информации и кодированию. Издательское объединение «Вища школа» Киев – 1976. 276 с.

4. Захарченко В.Н., Гайдар В.П., Улеев А.П., Липчанский А. И. Методы повышения эффективности использования каналов связи, м. Київ "Техніка", 1998.

5. Фано. Передача информации. Статистическая теория связи "Мир", 1965.

6. Гусєв О.Ю., Конохович Г.Ф., Корнієнко А.І. Теорія електричного зв'язку: навчальний посібник Львів: Магнолія 2006-2010, 364с.

Рецензент: Захарченко Н.В., д.т.н., проф., Одесская национальная академия связи им. А.С. Попова, г. Одесса, Украина

ПІДВИЩЕННЯ ПРИХОВАНОСТІ ПОВІДОМЛЕНЬ, ЩО ПЕРЕДАЮТЬСЯ, В СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

В.В. Гордійчук

У роботі розглянуто метод шифрування передаваємого тексту з використанням дозволених кодових множин з різними модулями рівняння якості з додатковою зміною номерів кодових символів у вихідній таблиці.

Ключові слова: *інформаційна безпека, інформаційна скритність, передача інформації, таймерні сигнальні конструкції, система залишкових класів*

RESIDUAL CLASSES SYSTEM WITH THE TIMER-SIGNAL CONSTRUCTIONS FOR THE CRYPTORESISTANCE INCREAS

V. Hordiichuk

Considers the method of transmitted text encryption using allowed code sets with different quality equation modules and additional code symbol numbers change in the source table

Key words: *information security, information secrecy, information transmission, timer-signal constructions, system of residual classes*