УДК 681.322, 681.51

Т.В.Жгун, Б.Ф.Кирьянов

МОДЕЛЬ СКРЫТНОЙ ПЕРЕДАЧИ ЦИФРОВОЙ ИНФОРМАЦИИ

The model of useful digital data transmission alternating with the random codes transmission, is suggested and investigated. It allows to raise reliability of data protection, when transmitting it by modern computer nets.

Идея спрятать двоичные символы полезной информации между передаваемыми случайными двоичными символами для бинарного канала связи предлагалась (но не исследовалась) в [1]. Реализация такой модели позволила бы повысить криптостойкость большинства известных методов защиты информации, допускающих несанкционированный прием передаваемых по каналу связи кодов, но практически исключающих расшифровку этой информации [2].

В данной работе предлагается и исследуется модель передачи кодов полезной информации со случайным чередованием их с передачей случайных кодов. По мнению авторов, такая модель актуальна для передачи информации по современным компьютерным сетям [3].

Рекомендуемая модель предусматривает:

1. Наличие в компьютерах сети, между которыми осуществляется обмен информацией, программных или аппаратных генераторов псевдослучайных кодов (ГПСК), выдающих на каждом шаге t работы модели n-разрядные коды

$$X(t) = A \cdot X(t-1), \tag{1}$$

где A — матрица над полем $GF(2^n)$, одинаковая для ГПСК всех указанных компьютеров в течение сеанса связи.

2. Ввод ГПСК всех компьютеров в синхронизм, т. е. обеспечение совпадения кодов $X(t)$ реализуемых алгоритмом (1), на каждом шаге работы всех ГПСК системы связи.

3. Обмен полезной информацией под управлением работающих в состоянии синхронизма ГПСК. При этом в случае появления в некоторой m-разрядной части кода $X(t)$ ($m < n$) заранее установленной ключевой кодовой комбинации $X_{кл}$ по каналу связи сети передается код полезной информации $K_{пи}(t)$. В противном случае осуществляется передача случайного или псевдослучайного кода.

Проанализируем задачу ввода в синхронизм k ГПСК компьютерной сети. Будем считать, что эта задача решается путем передачи синхронизирующим ГПСК кодов $X(t)$, начиная с момента $t = 0$ (t — число шагов работы модели). Поскольку в поступающей из каналов сети информации в общем случае могут быть ошибки (прием символов 0 вместо 1 и 1 вместо 0), то будем считать, что в компьютеры сети с настраиваемыми ГПСК вместо $X(t)$ может поступить код $X^*(t)$, который может отличаться от $X(t)$.

Переключение ГПСК в режим синхронизма предлагается производить при выполнении условия $X(t) = A \cdot X(t-1)$, проверяемого в приемниках информации на каждом шаге t. Тогда в случае выполнения условия $X^*(t) = A \cdot X^*(t-1)$ произойдет ошибочное переключения соответствующего ГПСК в режим синхронизма.

Для оценки работоспособности рассматриваемой системы передачи информации найдем зависимость вероятности $W_k(t)$ выполнения условия правильного переключения в режим синхронизма всех k настраиваемых ГПСК от параметров системы связи, а также

проанализируем возможность ошибочного переключения в режим синхронизма ГПСК рассматриваемой системы связи. Очевидно, правильное переключение всех ГПСК в режим синхронизма произойдет не позднее t при условии, что за это время ни один из них не будет переключен в режим синхронизма ошибочно.

Пусть вероятность правильного приема одного разряда кода $X(t)$ равна p, вероятность его неправильного приема — q, а появления рассматриваемых ошибок являются независимыми событиями. Поскольку для любого ГПСК условие ввода его в режим синхронизма в момент t выполняется при приеме кодов $X(t-1)$ и $X(t)$ и невыполнении условия ввода в синхронизм до момента t, то для вероятности $W_1(t)$ для $t \geq 3$ получаем:

$$W_1(t) = W_1(t-1) + [1 - W_1(t-1)] \cdot P_B \cdot p^n, \tag{2}$$

где n — число разрядов передаваемых кодов (кодов ГПСК), а P_B — Бейесова вероятность невыполнения условия входа в синхронизм в момент $t-1$ за счет приема $X^*(t-2)$ и $X(t-1)$, равная $p^n/(1+p^n)$. Причем $W_1(0) = W_1(1) = 0$, $W_1(2) = p^{2n}$. Приняв $P_B = 1$, можем распространить разностное уравнение (2) и на случай $t = 2$.

Решая уравнение (2) и учитывая, что $W_k(t) = [W_1(t)]^k$, находим:

$$W_k(t) = \left[1 - \left(1 - p^{2n}\right) \cdot \left(1 - \frac{p^{2n}}{1+p^n}\right)^{t-2}\right]^k, \quad t \geq 2. \tag{3}$$

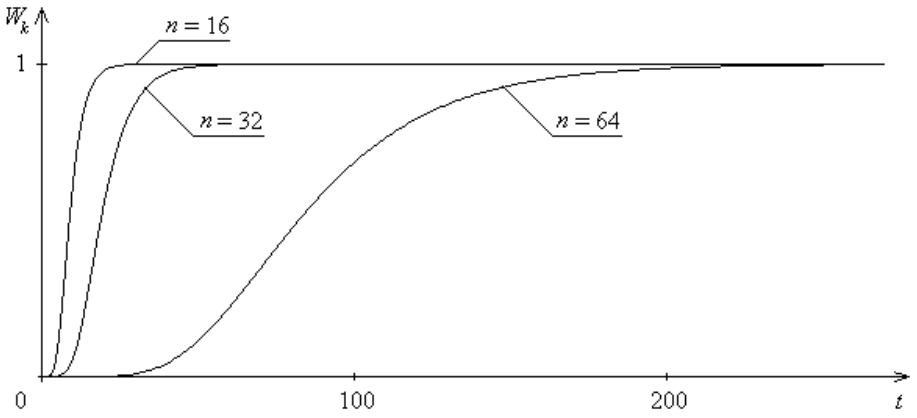

Рис.1. Графики функции $W_k(t)$ при $p = 0{,}95$, $n = 32$ и разных n.

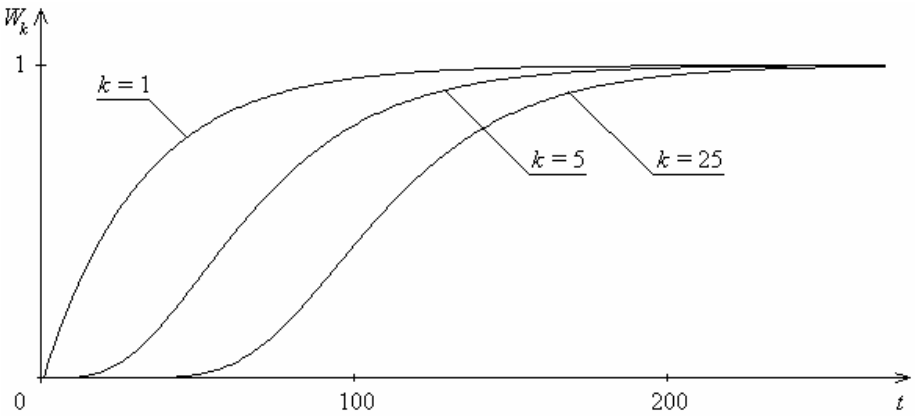

Рис.2. Графики функции $W_k(t)$ при $p = 0{,}95$, $n = 32$ и разных k

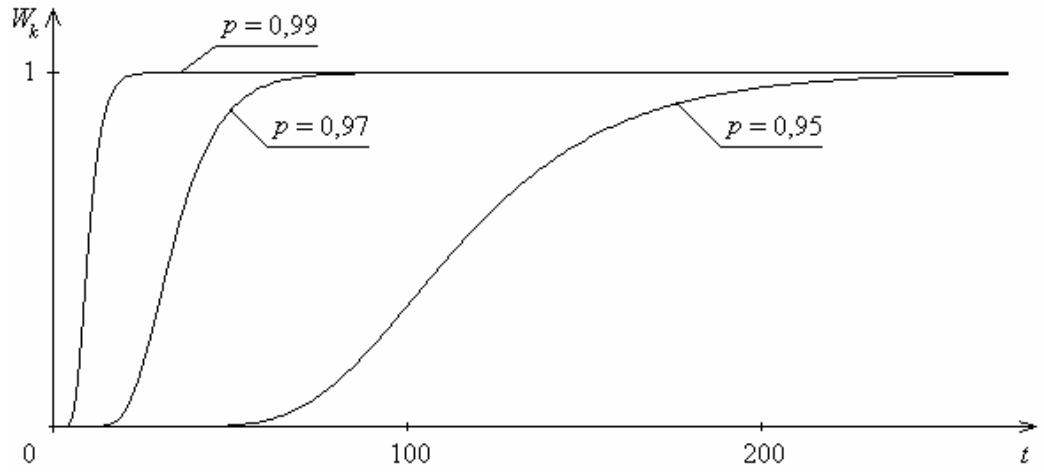

Рис.3. Графики функции $W_k(t)$ при $n = 32$, $k = 25$ и разных p

Графики на рис. 1-3 иллюстрируют зависимость вероятности W_k от времени при различных значениях параметров p, n и k. Из графиков можно заключить, что даже при весьма большой вероятности q неправильного приема двоичных символов из канала связи (значение $q = 1 - p = 0{,}05$ считается очень большим) вход в синхронизм с помощью предложенного алгоритма осуществляется быстро.

Если задано минимально допустимое значение $W_{\min}$, характеризующее надежность установления синхронизма всех ГПСК, то из выражения (3) можно найти соответствующее значение $t_{\min}^{(c)}$, гарантирующее заданную надежность:

$$t_{\min}^{(c)} = \operatorname{trunc}\left[2 + \frac{\ln\left(1 - \sqrt[k]{W_{\min}}\right) - \ln\left(1 - p^{2n}\right)}{\ln\left(1 + p^{n} - p^{2n}\right) - \ln\left(1 + p^{n}\right)}\right]. \qquad (4)$$

В случае, например, $P_{c\min} = 0{,}999$, $k = 5$, $n = 32$ и $p = 0{,}99$ получим $t_{\min}^{(c)} = 24$, а при $p = 0{,}95$ $t_{\min}^{(c)} = 268$, что для современных компьютерных систем является малой величиной.

Рассмотрим, наконец, возможность ошибочного переключения ГПСК в режим синхронизма. Эта задача анализировалась путем моделирования системы ГПСК, алгоритм работы (1) которых задавался матрицами A с примитивными собственными многочленами [4, 5]. В процессе моделирования находились оценки среднего времени $t_{\min}^{(o)}$ ошибочного переключения ГПСК в режим синхронизма при условии игнорирования сигналов о выполнении критерия (1) на настраиваемых ГПСК. Моделирование показало, что кроме параметров p, n и k на оценки $t_{\min}^{(o)}$ оказывает влияние вид матриц A и, в частности, вид собственных (характеристических) многочленов этих матриц.

В табл. приведены значения оценок $t_{\min}^{(o)}$, полученных путем моделирования процесса ввода в синхронизм одного 16-разрядного ГПСК при различных значениях p. Работа ГПСК задавалась матрицей с собственным многочленом $H(\lambda) = \lambda^{16} + \lambda^{15} + \ldots + \lambda^{5} + \lambda^{3} + \lambda^{2} + 1$. Объем испытаний для получения каждой оценки составлял 10^4 сеансов настройки, каждый из которых продолжался до первого выполнения условия $X^*(t) = A \cdot X^*(t-1)$.

Для сравнения в таблице приведены и значения $t_{\min}^{(c)}$, полученные из выражения (4) при тех же параметрах системы связи и $W_{\min}$= 0,99.

p	0,95	0,96	0,97	0,98	0,99	0,995
$t_{\min}^{(o)}$	748	758	802	1031	2191	6307
$t_{\min}^{(c)}$	33	24	18	13	9	5

Реально в компьютерных сетях вероятность ошибки при приеме одного символа передаваемого по каналу связи кода существенно меньше 0,01. Поэтому из данных таблицы можно сделать вывод, что вероятность ошибочного переключения ГПСК в режим синхронизма ничтожно мала, а ввод ГПСК в синхронизм согласно предложенному алгоритму может быть осуществлен путем передачи лишь нескольких кодов настраивающего ГПСК.

1. Кирьянов Б. Ф. Микропроцессорные средства в задачах имитации и обработки случайных сигналов. Ч. 2. Новгород: НПИ, 1989. 48 с.
2. Хоффман Л. Дж. Современные методы защиты информации. М.: Сов. радио, 1980. 264 с.
3. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999. 328 с.
4. Гилл А. Линейные последовательностные машины. М.: Наука, 1974. 288 с.
5. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М.: Мир, 1976. 596 с.