УДК 621.391

В.В. Корчинский[1]

[1] *к.т.н., доцент кафедры информационной безопасности и передачи данных, кандидат технических наук Одесская национальная академия связи им. А.С. Попова*

ПОВЫШЕНИЕ КАЧЕСТВЕННЫХ ХАРАКТЕРИСТИК КРИПТОСИСТЕМЫ МАКЭЛИСА

Предложен метод повышения качественных характеристик криптосистемы МакЭлиса. Показана возможность уменьшения избыточности шифрования и повышения информационной скрытности криптосистемы МакЭлиса при совместном использовании её с таймерными сигнальными конструкциями.
Ключевые слова: шифрование, таймерное кодирование, избыточность, криптосистема МакЭлис, шифрование ТСК.

Постановка проблемы в общем виде и ее связь с важными научными или практическими заданиями. Появление сетей передачи данных с высокой пропускной способностью и развитием мультимедиа-технологий создаёт проблему шифрования больших объемов информации. В XX веке основным типом шифруемых и передаваемых сообщений было текстовое сообщение, а в настоящее время возникла потребность в криптографической защите при передаче цифровых видео- и речевых сообщений, видеоконференций и т.д. Такое шифрование должно осуществляться в реальном режиме времени и с минимальной задержкой для пользователей. Это требование выдвигает решение проблемы по изысканию быстродействующих методов шифрования информации.

Анализ последних исследований и публикаций, в которых положено начало решение проблемы, выделения нерешенных вопросов общей проблемы. Эффективность конфиденциальной системы связи (КСС) целесообразно оценивать с помощью комплексного показателя качества – помехозащищенности [1], который включает понятия помехоустойчивости и скрытности.

Помехоустойчивость может быть обеспечена как путём применения эффективных способов приема и обработки сигналов, так и помехоустойчивым кодированием информации [2]. Оценивается помехоустойчивость с помощью интегрированного показателя качества – вероятности ошибки в приеме одного бита информации, на величину которой влияют помехи как естественного, так и искусственного происхождения (различного рода шумы, многолучевое распространение сигналов, преднамеренные помехи и т. п.).

Скрытность [3] – обобщенный показатель КСС, который характеризует способность обеспечивать безопасность и целостность хранящейся или циркулирующей информации в системе, сети или радиосети от НСД и учитывает различные их состояния и уровни защищенности. Скрытность можно классифицировать с учётом предмета поиска и преследуемой задачи противоборствующей стороны (станция несанкционированного доступа, разведки и радиопротиводействия). Различают информационную, структурную, энергетическую и другие показатели скрытности системы [1, 3].

Энергетическая скрытность характеризует способность системы противостоять мерам НСД, направленным на обнаружение сигнала и реализуется в основном на первом уровне модели OSI.

Структурная скрытность направлена на существенное затруднение раскрытия сигнала при условии, что сигнал средствами НСД уже обнаружен. Это означает распо-

знавание формы сигнала и измерение его параметров, т. е. отождествление обнаруженного сигнала с одним из множества априорно известных сигналов и реализуется чаще всего на втором уровне модели OSI [1].

Информационная скрытность [9] определяется способностью противостоять мерам, направленным на раскрытие смысла передаваемой с помощью сигналов информации и реализуется на старших уровнях модели OSI [1]. Реализуется информационная скрытность с помощью криптографических методов, которые должны обеспечивать защиту зашифрованной информации в основном только от одного вида разрушающих воздействий – предумышленного разрушения или искажения информации. Однако при передаче информации от абонента к абоненту возможны случайные помехи на линиях связи, ошибки и сбои аппаратуры, частичное разрушение носителей данных и т.д.

Хотя предназначение показателей помехоустойчивости и скрытности различно, однако при построении КСС приходится решать общие взаимосвязанные задачи, учитывающие алгоритм работы системы или сети, выбора метода защиты от ошибок, полосы пропускания канала связи, системы шифрования, процедуры доступа к ресурсам сети и т.д.

Среди рассмотренных показателей скрытности и помехоустойчивости можно выделить схожие преобразования, которые характерны как при криптографическом шифровании, так и помехоустойчивом кодировании – после обработки информация по определенному алгоритму меняет свою форму представления, но не теряет смысл. На практике эти два вида преобразования отчасти дополняют друг друга, и их комплексное использование помогает эффективно решать задачи надежной защиты передаваемой информации в канале связи от всех видов воздействия.

Очевидно, что увеличение быстродействия шифрования больших объемов информации в реальном режиме времени и с минимальной задержкой для пользователей возможно при объединении процедуры криптографического шифрования и помехоустойчивого кодирования в одну общую задачу. В теории криптосистем с открытым ключом известны два основных типа систем, которые реализованы на линейных кодах: система МакЭлиса (McElice) [4] и система Нидеррайтера [5]. В данной статье рассматривается система МакЭлиса.

Целью работы является *улучшение качественных характеристик криптосистемы МакЭлиса с помощью таймерного кодирования*.

Изложение основного материала. Криптосистема МакЭлис (R. McEliece) с открытым ключом была разработана в 1978 г. с использованием методов теории помехоустойчивого кодирования [4] и реализована на основе корректирующего кода, который известен как код Гоппы. Основная идея шифрования заключается в преобразовании информационного блока в линейный код без определенной структуры. Известен быстрый алгоритм декодирования кода Гоппы, однако существующий в настоящее время алгоритм поиска кодового слова по заданному весу в произвольном линейном двоичном коде имеет экспоненциальную трудоемкость [4].

Алгоритм криптографического преобразования заключается в следующем. Пусть $d_н(x, y)$ – кодовое расстояние Хэмминга между двоичными последовательностями x и y. Параметры n, k и t являются параметрами криптосистемы, где n – длина кодового блока, k – длина информационного кодового блока сообщения; t – кратность исправления ошибок. Секретный ключ состоит из трех частей: G' – порождающая матрица кода Гоппы, исправляющего t ошибок; P – матрица перестановок размером $n \times n$; S – невырожденная матрица размером $k \times k$. Открытым ключом служит матрица G размером $k \times n$: $G = SG'P$. Открытый текст преобразован в строку из k бит и представлен в виде k-элементного вектора поля $GF(2)$. Для шифрования сообщения случайным образом выбирается n-элементный вектор z над полем $GF(2)$, для которого расстояние Хэмминга меньше или

равно *t,* и вычисляется

$$c = mG + z\,.$$

Для дешифрования кодового слова сначала определяется c' = CP^{-1}'. Затем с помощью алгоритма декодирования для кодов Гоппы находится *m',* для которого $d_н(x, y)$ меньше или равно *t.* Далее вычисляется

$$m = m'S^{-1}\,.$$

Для криптосистемы МакЭлис были определены минимальные значения *n*=1024, *t*=50 и *k*=524 [4], при которых гарантируется адекватная криптостойкость шифра и обеспечивается быстродействие на два-три порядка выше, чем у криптосистемы с открытым ключом RSA. Однако главным недостатком криптосистемы МакЭлис является увеличение длины шифрованного текста почти в два раза, по сравнению с исходным информационным кодовым блоком, т.е. избыточность шифрования составляет 100%.

Для компенсации избыточности шифрования предлагается метод совместного применения криптосистемы МакЭлис с таймерным кодированием [6].

Теория таймерного кодирования была предложена в 80-х годах прошлого века и основное её научное внимание было акцентировано на вопросах повышения скорости передачи в бинарных каналах с ограниченной полосой и обеспечения требуемой помехоустойчивости [6]. Исследование, проведенные в [7,8], показали, что таймерные сигнальные конструкции можно использовать также и для задачи шифрования информации. Максимальная эффективность в этом случае может быть достигнута за счет совместного применения таймерных сигнальных конструкций (ТСК) и других систем шифрования.

Рассмотрим возможности ТСК по компенсации избыточности шифрования криптосистемы МакЭлис.

Пусть $n_{\text{тск}}$ – количество элементарных посылок, а t_0 – их длительность, тогда $T_{\text{с}} = n_{\text{тск}} t_0$ – интервал времени, на котором формируется сигнальная конструкция таймерного кода. При построении сигнальной конструкции используется базовый элемент $\Delta = t_0 / s$, где $s \in 1, 2, 3, \ldots, l$ – целые числа. В отличие от разрядно-цифрового кода (РЦК), когда информация о передаваемом разряде определяется уровнем сигнала элементарной посылки, в ТСК информация заложена в нескольких отдельных (временных) интервалах сигнала $t_{\text{с}} = t_0 + k\Delta$, где $k \in 0, 1, 2, \ldots, s \cdot (n_{\text{тск}} - 2)$ и их на интервале $T_{\text{с}}$ взаимном положении. С одной стороны такой метод формирования дает возможность передавать в канал отрезки сигнала длительностью $t_c \geq \Delta \cdot (s + i)$, где $i = 0, 1, 2, 3 \ldots$, что исключает межсимвольные искажения в каналах с базой $B = 1$. С другой стороны не кратность t_c величине t_0 позволяет уменьшить расстояние между сигнальными конструкциями до величины $\Delta < t_0$ и получить число реализаций ТСК $N_{\text{рТСК}}$ на интервале $n_{\text{тск}} t_0$ значительно больше 2^n [3]

$$N_{\text{рТСК}} = \sum_{i=1}^{n_{\text{тск}}} \frac{\left[\left(n_{\text{тск}} \cdot s\right) - \left[\left(s-1\right) \cdot i\right]\right]!}{i! \cdot \left[\left[\left(n_{\text{тск}} \cdot s\right) - \left[\left(s-1\right) \cdot i\right]\right] - i\right]!}\,. \qquad (1)$$

В табл. 1 приведено число реализаций ТСК с учетом значений s, $n_{\text{тск}}$ и $i = 1 \ldots n_{\text{тск}}$. Как видно из табл. 1 такой метод позволяет сформировать значительно больше разрешенных ТСК на одном и том же интервале, чем кодовых слов РЦК, где число реализаций $N = 2^{n_{\text{тск}}}$. Например, при формировании ТСК на интервале $T_c = 5t_0$ и $s = 7$ число возможных реализаций $N_{\text{рТСК}} = 1293$. Такое количество

реализаций можно получить только с помощью простого двоичного кодового слова с длиной $n = \lceil \log_2 1293 \rceil = 11$ элементов. На рис. 1 приведен пример формирования нескольких реализаций бинарных ТСК на интервале времени $T_c = 4t_0$ при базовом элементе Δ.

Таблица 1

Количество реализаций ТСК $N_{\text{рТСК}}$ при различных значениях s и n.

n \ s	1	2	3	4	7	10	15	20
5	31	88	188	344	1293	3310	10475	24940
8	255	1596	5895	16492	153400	735450	4952841	20628612
10	1023	10945	58424	217224	3705000	27042520	$3{,}02 \cdot 10^8$	$1{,}83 \cdot 10^9$

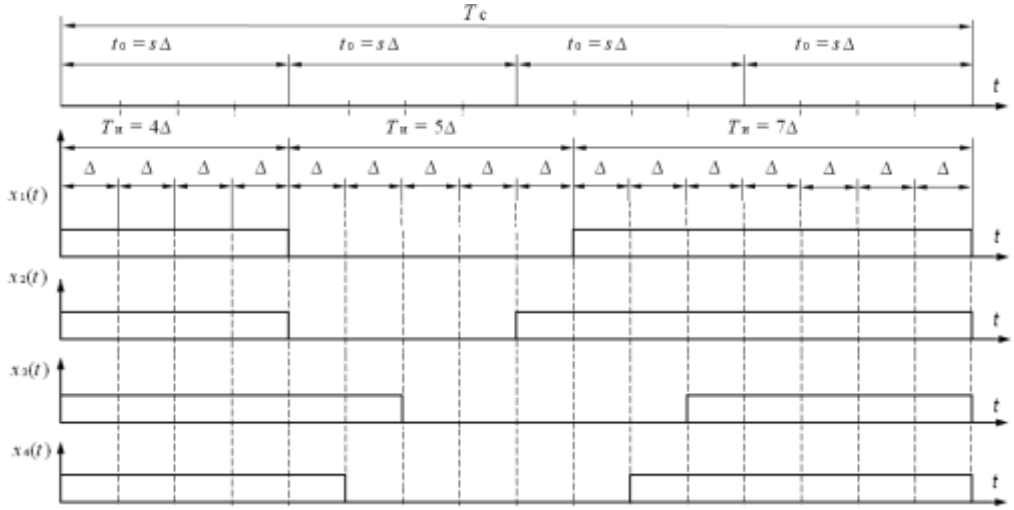

Рисунок 1 − Формирование реализаций ТСК на интервале времени $T_c = 4t_0$ при базовом элементе Δ

На рис. 2 показана упрощенная структурная схема системы передачи конфиденциальной информации с использованием криптосистемы МакЭлис и ТСК. Источник информации (ИИ) выдает непрерывную последовательность информационных двоичных элементов РЦК длины $k_{\text{сл}}$=8, которые формируется в блоки $k = k_{\text{сл}} N$, где N – количество кодовых слов $k_{\text{сл}}$. Для криптосистемы МакЭлис k=524 разрядов, что обеспечит шифрование 65 информационных кодовых слов $k_{\text{сл}}$=8. После шифрования длина кодового блока составит $n_{\text{ш}}$=1024. Далее кодеком ТСК блок $n_{\text{ш}}$ разбивается на отдельные блоки некоторой длины $k_{\text{РЦК}}$. Длина блока $k_{\text{РЦК}}$ определяется из условия максимального возможного числа реализаций $N_{\text{рТСК}}$, сформированных на некотором интервале n при выбранных значениях s и i, тогда

$$k_{\text{РЦК}} \le \log_2 N_{\text{рТСК}}. \qquad (2)$$

Каждой длине блока $k_{\text{РЦК}}$ соответствует число, определяющее номер реализации РЦК. Кодер ТСК осуществляет кодирование шифрованного сигнала РЦК $S_{\text{РЦК}}$ в сигнал ТСК $S_{\text{ТСК}}$ по правилу

$$S_{\text{РЦК}j} \rightarrow S_{\text{ТСК}z}(n, s, i), \tag{3}$$

т.е. каждый сигнал $S_{\text{РЦК}j}$ представляется определенной конструкцией $S_{\text{ТСК}z}$., где j и z − соответственно номера реализаций.

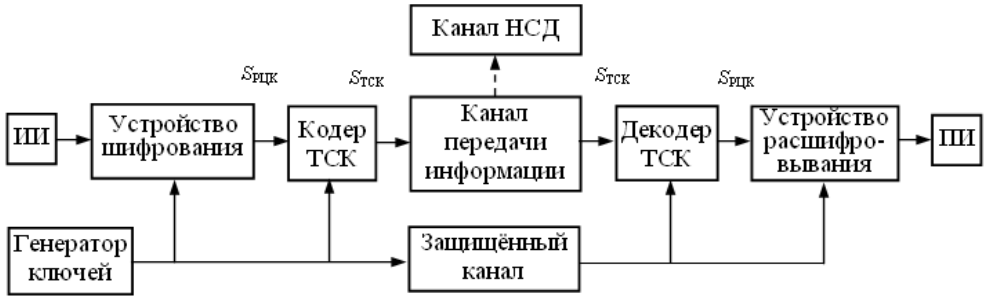

Рисунок 2 − Упрощенная структурная схема системы передачи конфиденциальной информации

При значениях $s = 3...7$ для $k_{\text{РЦК}}$=8 можно получить снижение избыточности шифрования криптосистемы МакЭлис от 30 до 115%. Выбор значений s рассмотрен в [6] и осуществляется с учетом качества канала и требуемой помехоустойчивости.

Изменение значений параметров n, s и i дает возможность на выходе кодера ТСК получать различные множества сигнальных конструкций, каждое из которых может отличаться длительностями, зависящими от значений n, числом базовых элементов s и числом переходов i, т. е. структурой сигнала. Например, при определенных значениях n и s можно формировать различные множества конструкций $S_{\text{ТСК}z}$ изменением только числа переходов i, где каждому его значению будет соответствовать множество со своей структурой сигнала. Аналогично, изменением s и n или различных допустимых комбинаций n, s, i можно на выходе кодера ТСК получать множества $S_{\text{ТСК}z}$ с разной формой сигнала. Частота смены параметров кодером ТСК выбирается такой, чтобы объем перехваченных станцией НСД реализаций ТСК определенной формы был недостаточен для раскрытия структуры сигнала в пределах интервалов времени, представляющих практический интерес. Так как параметры n, s и i должны быть известны приемной стороне, то их передача обычно осуществляется по отдельному достаточно защищенному каналу.

Выводы. В заключение следует отметить, что совместное использование шифрования и таймерного кодирования позволяет в зависимости от параметров n, s и i уменьшать избыточность криптосистемы МакЭлис. Кроме того, применяя шифрование ТСК, можно дополнительно повысить информационную и структурную скрытность передаваемых сообщений [7,8].

Литература

1. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты / В.И. Борисов, В.М. Зинчук, А.Е. Лимарев и др.; под ред. В.М. Борисова. – М.: Радио и связь, 2000. – 384 с.
2. Захарченко М. В. Системи передавання даних. Том 1. Завадостійке кодування / Захарченко М. В. – Одеса: Фенікс, 2009. – 447 с.

3. Каневский З. М. Теория скрытности / З. М. Каневский, В.П. Литвиненко – Воронеж : ВГУ, 1991. – 144 с.
4. McElice R.J. A Public Key Cryptosystem Based on Algebraic Coding Theory // DSN Progress Report 42–44. — Pasadena, CA: Jet Propulsion Lab, 1978. — P. 114–116.
5. 2. Niederreiter H. Knapsack-Type Cryptosystem and Algebraic Coding Theory // Probl. Control and Inform. Theory. — 1986. — V. 15. — P. 19–34.
6. Захарченко Н. В. Основы кодирования: учебное пособие / Н. В. Захарченко, А. С. Крысько, В. Н. Захарченко – Одесса: УГАС им. А.С. Попова, 1999. – 240 с.
7. Захарченко, Н. В. Структурная скрытность таймерных сигналов в системах с кодовым разделением каналов / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Восточно-Европейский журнал передовых технологий. – 2011. – № 2/9(50). – С. 7–9.
8. Захарченко, Н. В. Эффективность использования таймерных сигнальных конструкций в системах передачи с кодовым разделением каналов / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Наукові праці ДонНТУ. – 2011. – Випуск № 20(182). – С. 145–151.
9. Шаньгин, А.И. Информационная безопасность компьютерных систем и сетей [Текст] / А.И. Шаньгин. – М.: ИД «Форум»: ИФРА-М, 2008. – 416 с.

Надійшла до редколегії 27.03.2013 р.

Рецензент: д.т.н., проф. Петров А.С.

В.В. Корчінскій

ПІДВИЩЕННЯ ЯКІСНИХ ХАРАКТЕРИСТИК КРИПТОСИСТЕМИ МАКЭЛИСА

Запропоновано метод підвищення якісних характеристик криптосистеми Макеліс. Показано можливість зменшення надмірності шифрування і підвищення інформаційної скритності криптосистеми Макеліс при спільному використанні її з таймерного сигнальними конструкціями.

Ключові слова: шифрування, таймерного кодування, надмірність, криптосистема Макеліс, шифрування ТСК.

V.V. Korchinskiy

INCREASE OF THE QUALITATIVE CHARACTERISTICS OF CRYPTOSYSTEM OF MAKELIS

A method of increasing the quality characteristics of the McEliece cryptosystem is proposed. The possibility of reducing the redundancy of the encryption and increasing information secrecy McEliece cryptosystem when used it with the timed signal designs.

Keywords: enciphering, timer coding, redundancy, cryptosystem Makelis, TSK enciphering.