УДК 621.391

РАЗРАБОТКА АЛГОРИТМА ФОРМИРОВАНИЯ КОДОГРАММ В КАСКАДНЫХ ТЕОРЕТИКО-КОДОВЫХ СХЕМАХ

В.И. Грабчак
(Сумской военный институт РвиА)

Предлагается алгоритм формирования кодограмм в каскадных теоретико-кодовых схемах (ТКС), построенных на обобщенных каскадных кодах. Проводится оценка временно́й и емкостно́й сложности его реализации.

системы теоретической стойкости, алгебраические блоковые коды, каскадные теоретико-кодовые схемы

Постановка проблемы в общем виде и анализ литературы. Важными требованиями к качеству передачи данных в АСУВ является достоверность и информационная скрытность [1 – 2]. В работе [3] показано, что эффективным механизмом комплексного обеспечения указанных требований являются секретные системы, задача взлома которых сводится к известной в теории помехоустойчивого кодирования теоретико-сложностной задаче декодирования случайного кода. Также показано, что наиболее эффективными, по соотношениям длины ключа, обеспечиваемой стойкости и сложности реализации являются каскадные ТКС, построение которых базируется на маскировании кодов внешней ступени обобщенного каскадного кода. **Целью статьи** является разработка алгоритма формирования кодограмм в каскадных ТКС, оценка временно́й и емкостно́й сложности его реализации.

Разработка алгоритма формирования кодограмм в каскадных ТКС. Для построения алгоритма формирования кодограмм в каскадных ТКС воспользуемся алгебраическим описанием обобщенных каскадных кодов [4]. По определению алгебраически заданный обобщенный каскадный код порядка m однозначно определяется n_2 квадратными двоичными матрицами H_0^j, $j=\overline{1,n_2}$ порядка n_1 (задающих (n_1, k_i, d_{1i}) коды первой ступени) и $m+1$ групповыми над $GF(2^{a_i})$, $i=\overline{1,m+1}$ кодами второй ступени с параметрами (n_2, b_i, d_{2i}).

Согласно введенному в [4] определению каскадная ТКС формируется путем маскировки кодов внешней ступени, а процесс формирования кодограмм соответствует формированию кодового слова замаскирован-

ного каскадного кода с добавлением к нему случайного вектора ошибки. В этом случае алгоритм формирования кодограмм в общем виде можно представить в виде последовательности следующих шагов.

Шаг 1. Ввод и подготовка ключевых данных $K_i = \{G_X^1, G_X^2, ..., G_X^{m+1}\}$, параметризирующих прямое отображение в каскадной ТКС, где K_i – множество генераторных матриц, которые задают m+1 замаскированных кодов внешней ступени $G^i{}_X = X^i \cdot G^i \cdot P^i \cdot D^I$; X^i, P^i и D^i – хранящиеся в секрете маскирующие матрицы.

Шаг 2. Ввод информационного блока данных

$$M_i = \{(I_{1,1}, I_{1,2}, ..., I_{1,a_1}), (I_{2,1}, I_{2,2}, ..., I_{2,a_1}), ..., (I_{b_1,1}, I_{b_1,2}, ..., I_{b_1,a_1}),$$

$$...$$

$$(I_{1,1}, I_{1,2}, ..., I_{1,a_{m+1}}), (I_{2,1}, I_{2,2}, ..., I_{2,a_{m+1}}), ..., (I_{b_{m+1},1}, I_{b_{m+1},2}, ..., I_{b_{m+1},a_{m+1}})\}.$$

Шаг 3. Формирование кодового слова обобщенного каскадного кода

$$C_i = \{(C_{1,1}, C_{1,2}, ..., C_{1,a_1}), (C_{2,1}, C_{2,2}, ..., C_{2,a_1}), ..., (C_{n_2,1}, C_{n_2,2}, ..., C_{n_2,a_1}),$$

$$...$$

$$(C_{1,1}, C_{1,2}, ..., I_{1,a_{m+1}}), (C_{2,1}, C_{2,2}, ..., C_{2,a_{m+1}}), ..., (C_{n_2,1}, C_{n_2,2}, ..., C_{n_2,a_{m+1}})\}$$

или $C_i = \{(\gamma_{1,1}, \gamma_{1,2}, ..., \gamma_{1,n_2}), (\gamma_{2,1}, \gamma_{2,2}, ..., \gamma_{2,n_2}), ..., (\gamma_{m+1,1}, \gamma_{m+1,2}, ..., \gamma_{m+1,n_2})\}$, где $\gamma_{i,j} = (C_{j,1}, C_{j,2}, ..., C_{j,a_i})$.

Шаг 4. Формирование случайного вектора ошибки (случайного сеансового ключа)

$$e_i = \{(e_{1,1}, e_{1,2}, ..., e_{1,n_2}), (e_{2,1}, e_{2,2}, ..., e_{2,n_2}), ..., (e_{m+1,1}, e_{m+1,2}, ..., e_{m+1,n_2})\},$$

так, что e_{ij} – двоичный вектор длины a_i, или $e_{ij} \in GF(2^{a_i})$, причем для всех $i = 1,..,m+1$ выполняется условие

$$w(e_{i,1}, e_{i,2}, ..., e_{i,n_2}) \le t_{2i} = (d_{2i} - 1)/2. \qquad (1)$$

Шаг 5. Формирование кодограммы E_i путем прибавления (в арифметике поля $GF(2^{a_i})$) к вектору C_i сеансового ключа e_i:

$$E_i = \{(\gamma^*_{1,1}, \gamma^*_{1,2}, ..., \gamma^*_{1,n_2}), (\gamma^*_{2,1}, \gamma^*_{2,2}, ..., \gamma^*_{2,n_2}), ..., (\gamma^*_{m+1,1}, \gamma^*_{m+1,2}, ..., \gamma^*_{m+1,n_2})\},$$

где $\gamma^*_{ij} = \gamma_{ij} + e_{ij}$, а γ_{ij} и e_{ij} – двоичные вектора длины a_i.

Последовательное выполнение шагов предложенного алгоритма позволяет за конечное число операций сформировать кодограмму в каскадной ТКС, заданной по обобщенному каскадному коду.

Исследование сложности реализации предложенного алгоритма. В соответствии с основными положениями теории сложности время, затрачиваемое алгоритмом, как функция размера задачи, называется временно́й

сложностью этого алгоритма. Аналогично определяется емкостна́я сложность алгоритма. Проведем оценку временно́й и емкостно́й сложности разработанного алгоритма формирования кодограмм.

Анализ предложенного алгоритма показывает, что при условии предварительного ввода и подготовки ключевых данных (шаг 1) и предварительного формирования сеансового ключа (шаг 4) формирование кодограммы состоит в формировании кодового слова обобщенного каскадного кода и наложении сеансового ключа. Сложность реализации алгоритма формирования кодового слова обобщенного каскадного кода как функция размера задачи определяется суммой сложностей реализации алгоритмов кодирования кодами внешней и внутренней степеней обобщенного каскадного кода. Предположим, что при реализации алгоритма в памяти сберегаются элементы порождающих матриц всех кодов первой и второй ступени. Тогда на i-м временном интервале при выполнении третьего шага алгоритма формирования кодограмм производится операция кодирования i-м кодом внешней и/или внутренней ступени. Всего необходимо выполнить кодирование $m + 1$ кодами внешней и внутренней ступени, т.е. временна́я сложность алгоритма составит

$$S_B = 2(m + 1) \tag{2}$$

временных интервалов. Емкостна́я сложность (двоичных ячеек памяти):

$$S_E = n_2 \sum_{i=1}^{m+1} (b_i \cdot a_i + k_i). \tag{3}$$

Предположим, что при реализации алгоритма в памяти сберегаются только элементы порождающих многочленов (для циклических кодов). Степень порождающего многочлена (n_2, b_i, d_{2i}) кода второй ступени равна

$$r_{2i} = n_2 - b_i.$$

Степень порождающего многочлена (n_1, k_i, d_{1i}) кода 1-й ступени равна

$$r_{1i} = n_1 - k_i.$$

Тогда при выполнении 3-го шага алгоритма формирования кодограмм необходимо реализовать умножение порождающего многочлена на информационный многочлен, соответствующий введенной информационной последовательности. Процедура умножения двух многочленов может быть легко реализована, например, с помощью регистров сдвига и потребует, соответственно, r_{2i} и/или r_{1i} операций сдвига и сложения. Всего, для реализации алгоритма кодирования обобщенного каскадного кода потребуется

$$S_B = 2(m+1)(n_2 + n_1) - 2\sum_{i=1}^{m+1} (b_i + k_i) \tag{4}$$

временных интервалов. Емкостна́я сложность (двоичных ячеек памяти):

$$S_E = \sum_{i=1}^{m+1} (b_i \cdot a_i + k_i). \tag{5}$$

Процедура наложения сеансового ключа состоит в добавлении к кодовому слову обобщенного каскадного кода случайного вектора ошибок, удовлетворяющего условию (1). Процедура сложения двух векторов длины n_2 может быть реализована за один временно́й интервал и потребует n_2 ячеек памяти. Всего, с учетом (2), (3) временна́я сложность алгоритма формирования кодограмм в каскадной кодовой схеме защиты информации составит

$$S_B = 3(m + 1) \qquad (6)$$

временных интервалов. Емкостна́я сложность (двоичных ячеек памяти):

$$S_E = n_2 \sum_{i=1}^{m+1} (b_i \cdot a_i + k_i + n_2 \cdot a_i) . \qquad (7)$$

Для выражений (4), (5) окончательные соотношения примут вид

$$S_B = 2(m+1)(n_2 + n_1) + (m+1) - 2\sum_{i=1}^{m+1} (b_i + k_i) \qquad (8)$$

временных интервалов. Емкостна́я сложность (двоичных ячеек памяти):

$$S_E = \sum_{i=1}^{m+1} (b_i \cdot a_i + k_i + n_2 \cdot a_i) . \qquad (9)$$

Выводы. Предложен алгоритм формирования кодограмм в каскадных ТКС, который основан на последовательном выполнении процедуры маскирования обобщенного каскадного кода и процедуры кодирования соответствующего кодового слова, что позволяет за конечное число шагов сформировать кодограмму и интегрировано обеспечить достоверность и информационную скрытность передачи данных в АСУВ. Проведенное исследование сложности реализации предложенного алгоритма показало, что показатели временно́й и емкостно́й сложности имеют полиномиальную зависимость от параметров обобщенного каскадного кода. **Перспективным направлением дальнейших исследований** является разработка практических рекомендаций по использованию разработанных предложений для повышения достоверности и информационной скрытности передачи данных в АСУВ.

ЛИТЕРАТУРА

1. *ДСТУ В 3265 – 95. Зв'язок військовий. – К.: УкрНДІССІ, 1995. – 23 с.*
2. *Науменко М.І., Стасєв Ю.В., Кузнецов О.О. Теоретичні основи та методи побудови алгебраїчних блокових кодів. Монографія. – Х.: ХУ ПС, 2005. – 267 с.*
3. *Кузнецов А.А., Грабчак В.И., Евсеев С.П. Каскадные кодовые схемы защиты информации // Системи обробки інформації. – Х.: ХУ ПС, 2005. – Вип. 9 (49). – С. 206-211.*
4. *Блох Э.Л., Зяблов В.В. Обобщенные каскадные коды. – М.: Связь, 1976. – 240 с.*

Поступила 5.01.2006

Рецензент: доктор технических наук, профессор Ю.В. Стасев,
Харьковский университет Воздушных Сил им. И. Кожедуба.