В. О. Осипян, **В. В. Подколзин** (Краснодар, КубГУ). **Об одной модификации рюкзачных систем защиты информации с открытым ключом.**

Пусть $A = (a_1, a_2, \ldots, a_n)$ — обобщенный рюкзачный вектор в $Z_p = \{0, 1, \ldots, p-1\}$, $p \neq 1$, $p \in N$, размерности n ($n \geqslant 3$), состоящий из n различных натуральных чисел [2].

О п р е д е л е н и е 1. Вектор $\Delta A = (\delta_1, \delta_2, \ldots, \delta_n)$ будем называть *вектором изменений вектора A в Z_p*, если выполняются следующие соотношения:

$$\delta_1 = a_1, \quad \delta_i = a_i - (p-1)\sum_{j=1}^{i-1} a_j, \qquad i = 2, \ldots, n. \tag{1}$$

Из (1) следует определение стандартного рюкзачного вектора, данного в [3]. В классической рюкзачной задаче защиты информации с открытым ключом в качестве открытого ключа используется вектор B, полученный из рюкзака A сильным модульным умножением. Как известно, такого типа СЗИ обладают слабой криптостойкостью [1].

Приведем модификацию рюкзачной СЗИ с открытым ключом, которая обладает более высокой степенью криптостойкости. Рассмотрим функциональный вектор $F = (f_1(x), f_2(x), \ldots, f_n(x))$, компоненты которого являются всюду определенными целочисленными функциями.

О п р е д е л е н и е 2. Пару (F, x_0) будем называть *генератором вектора* $B = (b_1, b_2, \ldots, b_n)$, если $b_i = f_i(x_0)$, $i = 1, \ldots, n$.

Определим модель СЗИ с открытым ключом следующим образом: 1) секретным ключом является функциональный вектор $F = (f_1(x), f_2(x), \ldots, f_n(x))$; 2) открытым ключом является x_0; 3) (F, x_0) является генератором вектора изменений ΔA рюкзака A в Z_p.

Функционирование предложенной модели: для заданного входа v определяется случайное число x_0; рассматривая (F, x_0) как генератор вектора ΔA, определяется рюкзак A; вычисляется криптотекст $w = (A, v)$; пара (x_0, w) публикуется отправителем; легальный получатель, на основе секретного ключа F и открытого ключа x_0, определяет A и находит v.

Очевидно, что криптостойкость системы значительно повышается, т. к. даже если криптоаналитик имеет информацию о природе вектора F, сами $f_i(x)$ ему не известны, и для каждой пары (x_0, w) необходимо решать NP-полную задачу о рюкзаке.

В заключение заметим, что если все компоненты $f_i(x)$ вектора F являются положительными функциями, то рюкзак A предложенной модели суть сверхрастущий.

СПИСОК ЛИТЕРАТУРЫ

1. *Саломаа А.* Криптография с открытым ключом. М.: Мир, 1995.
2. *Осипян В. О.* Разработка методов построения систем передачи и защиты информации. Краснодар, 2003.
3. *Коблиц Н.* Курс теории чисел и криптографии. М.: ТВП, 2001.