

В. О. О с и п я н, С. Г. С п и р и н а, А. В. О с и п я н (Краснодар, КубГУ). **Управление процессами стабилизации систем экономической информации.**

В условиях стремительного развития компьютерных, сетевых и телекоммуникационных технологий, включая технологии мобильной связи, крайнюю остроту приобретают проблемы защиты информации, в частности, экономической информации, что особенно остро прослеживается в банковском секторе, на всех ее уровнях хранения, обработки и передачи по каналам связи. Слабая практическая проработка положений по моделированию стабильных систем и процессов обеспечения защиты экономической информации, а также выбора оптимальных средств защиты обусловили содержание данной работы. В ней разрабатываются новые и применяются известные (например, с помощью задачи полной факторизации или других NP-полных задач, в частности, задач о рюкзаке и др.) методы для решения указанной проблемы на основе кольца целых гауссовых чисел. Учитывается, что в нем натуральные простые числа вида $4n + 3$ неразложимы, а числа $4n + 1$ разложимы [1].

Так, рассматривается система, аналогичная RSA [2] в основе которой лежит арифметика и алгоритм построения функций прямого $F(t) = t^L \bmod (n)$ и обратного $F^{-1}(c) = c^S \bmod (n)$ преобразований в кольце целых комплексных чисел, если каждому элементарному сообщению сопоставить комплексное число $a + bi$.

Так, например, открытый текст $T = \text{Six o'clock}$ с числовыми эквивалентами: $1 + 5i(S), 2 + 7i(i), 3 + 11i(x), 6 + 7i(o), 9 + 5i(c), 8 + 3i(l), 11 + 7i(k)$ с использованием открытого ключа $K_E = \{5, 65\}$ принимает вид: $E = 61\ 45\ 26\ 64\ 21\ 11\ 34\ 18\ 19\ 20\ 6\ 64\ 1\ 27\ 11\ 35\ 4\ 43$. Далее, используя секретный ключ $K_D = \{29, 65\}$, получаем последовательность $E' = 16\ 15\ 26\ 64\ 21\ 46\ 34\ 18\ 54\ 50\ 41\ 64\ 1\ 27\ 46\ 55\ 49\ 23$, которой соответствует текст T . В данном примере в качестве элементарных сообщений выступают буквы латинского алфавита.

В работе предлагаются также различные системы защиты экономической информации, в основе которых лежит трудная задача полной факторизации большого составного числа при неизвестных заранее простых его множителях в кольце целых гауссовых чисел. Для них разработан алгоритм построения и оперирования с большими числами.

В частности, разрабатываются СЗИ на основе различных вариантов задач о рюкзаке [2]. Так, например, для СЗИ на основе специального рюкзака разработан метод, который предлагает аналитику оперировать с высокими степенями при восстановлении открытого текста — в отличие от правомерного пользователя.

СПИСОК ЛИТЕРАТУРЫ

1. *Окунев Л. Я.* Целые комплексные числа. М.: 1941, 52 с.
2. *Осипян В. О., Осипян К. В.* Математические основы теории и практики защиты информации. Краснодар, КубГУ, 2003, 190 с.