ШИФРОВАНИЕ ДАННЫХ НА БАЗЕ РЕШЕНИЯ ЗАДАЧИ НАБЛЮДЕНИЯ ДИНАМИЧЕСКИХ СИСТЕМ

Ворона Е. В.

УО «Гродненский государственный университет им. Я. Купалы», Гродно, Беларусь, e-mail:voronaev93@gmail.com

В докладе обсуждается возможность использования известных результатов математической теории управления в криптографии и построения с ее помощью системы шифрования данных.

Вначале приведем некоторые известные факты, связанные с задачей наблюдения линейных дифференциальных систем. Предположим, что объект описывается линейным автономным дискретным уравнением:

$$x_{k+1} = Ax_k,\ k = 0, 1, \ldots \quad (1)$$

где x_k – n-вектор решения уравнения (1) $A \in R^{n\times n}$.

Так же предположим, что уравнение (1) снабжено известным выходом

$$y_k = Cx_k,\ k = 0, 1, \ldots \quad (2)$$

где $C \in R^{l\times n}(l < n)$.

Известно, что если rank[C', $A'C'$, $(A')^{n-1}C$,] = n где символ штрих обозначает операцию транспонирования), то существует операция восстановления неизвестного начального вектора x_0 по результатам известного выхода $Y = col[y0, \ldots, y_{n-1}]$, которую можно представить в виде:

$$x_0 = VY \quad (3)$$

где V – некоторая постоянная матрица соответствующего размера. Основная идея исследования - создание системы шифрования, которая по каналу передает вектор Y, а процесс дешифрования заключается в реализации операции (3).

В качестве ключей используются матрицы $A1$, $C1$, T.

Основная идея заключается в следующем. В качестве текста, который следует передать, берутся компоненты вектора x_0. Далее для пары матриц $A1$, $C1$ строится операция вида (3) (при $A=A1$, $C=C1$). После этого осуществляется переход к новому базису, определяемую матрицей T, в котором вычисляется вектор Y и передается получателю. Получатель посредством операции (3) проводит дешифровку. Разработан способ выбора матриц, позволяющий проводить описанный процесс шифрования/дешифрования в множестве целых чисел. Предполагается, что данная система шифрования наиболее эффективна для реализации числовой подписи, в качестве ее апробации построена соответствующая программная реализация алгоритма.

Литература