зуются ключи размером ~2^{2048}) и подверженность частотному криптоанализу (каждое значение после шифрования принимает только одно другое для данной пары ключей).

Как результат работы была написана программа для шифрования файлов на основе упрощенного варианта алгоритма Вернама, ключ которого шифруется алгоритмом RSA и встраивается в файл. Возведение в степень по модулю заданного числа реализовано бинарным алгоритмом как показавшим наибольшую производительность[2].

ЛИТЕРАТУРА

1. Криптология: учебник / Ю. С. Харин [и др.]. – Минск: БГУ, 2013. – 511 с.

2. Ишмухаметов, Ш. Т. Методы факторизации натуральных чисел: учебное пособие / Ш. Т. Ишмухаметов. – Казань: Казан. ун-т, 2011. – 190 с.

УДК 630.36

Студ. П.А. Струневский
Науч. рук. доц. В.В. Игнатенко
(кафедра высшей математики,БГТУ)

ДИНАМИЧЕСКОЕ ПРОГРАММИРОВАНИЕ В ЛЕСНОЙ ПРОМЫШЛЕННОСТИ

В лесной экономике, технологии и технике есть задачи, в которых необходимо учитывать изменения параметров систем во времени. Например, требуется провести дорогу, чтобы затраты на сооружение участка были минимальны.

Искусственно отрезок [L, M] между складами разделим на m частей, проведем через точки деления перпендикулярные прямые данному отрезку и будем считать на каждом шагу участок пути прямолинейным. Если разделить площадку на 5 частей, то получиться m=5+5=10 участков, направленных на север или восток. Проставим на каждом из отрезков число, выражающее затраты на строительство дороги на этом участке (рис.1).

Будем рассматривать сооружаемую дорогу как управляемую систему. Состояние этой системы перед началом каждого шага будет характеризоваться двумя координатами: восточной (x) и северной (y). Для каждого состояния системы (точки сетки) необходимо найти условное оптимальное управление так, чтобы затраты всех оставшихся до конца шагов (включая данный) были минимальными.

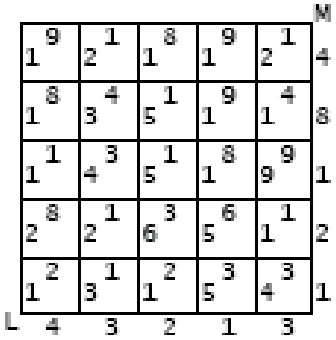

Рисунок 1 – Затраты на сооружение отдельных участков дороги

Процедуру условной оптимизации будем разворачивать в обратном направлении – от M к L. Начинаем с последнего шага. Минимальными затраты являются, если двигаться на восток (→, затраты 1 единица). Следующий шаг с минимальными затратами будет, если двигаться на север (↑, затраты 2 единицы). Мы выбираем такой шаг, чтобы итоговые затраты были минимальными. Проведя множество операций выбора шагов, возможными вариантами для постройки дороги с минимальными затратами являются два управления: 1 – (↑,↑,↑,→,→,→,↑,↑) и 2 – (↑,↑,↑,→,→,→,→,↑,↑,→).

УДК 51-72

Студ. Д.А. Бутницкая, студ. А.И. Чирвинский
Науч. рук. зав. кафедройО.Н. Пыжкова
(кафедра высшей математики, БГТУ)

ДВИЖЕНИЕ ТЕЛА ПЕРЕМЕННОЙ МАССЫ

В природе и технике нередки случаи, когда масса тел изменяется с течением времени за счет потери или приобретения вещества. Уравнения движения тел переменной массы являются следствием законов Ньютона, тем не менее, эти уравнения представляют самостоятельный интерес, главным образом как теоретическая основа ракетной техники.

Принцип действия ракеты очень прост[1]. Ракета с большой скоростью выбрасывает вещество (газы), воздействуя на него с большой силой. Выбрасываемое вещество с той же, но противоположно направленной силой в свою очередь действует на ракету и сообщает ей ускорение в противоположном направлении. На ракету действуют внешние силы: сила земной тяжести, гравитационное притяжение Солнца и планет, а также сила сопротивления среды, в которой движется ракета.