При заданных касательных напряжениях сил трения $\tau_м$ на границе раздела границе жидкость-газ, получим профиль скорости пленки жидкости:

$$\omega = \frac{\rho g \delta^2}{\mu}\left(\frac{x}{\delta} - \frac{1}{2}\cdot\frac{x^2}{\delta^2} - \frac{\tau_м}{\rho g \delta}\cdot\frac{x}{\delta}\right), \quad (3)$$

Находим среднюю скорость движения пленки

$$\omega_{ср} = \frac{1}{\delta}\int_0^{\delta}\omega dx = \frac{\rho g \delta}{\mu}\int_0^{\delta}\left(\frac{x}{\delta} - \frac{1}{2}\cdot\frac{x^2}{\delta^2} - \frac{\tau_м}{\rho g \delta}\cdot\frac{x}{\delta}\right)dx = \frac{\rho g \delta^2}{\mu}\left(\frac{1}{3} - \frac{\tau_м}{2\rho g \delta}\right), \quad (4)$$

Зависимости (3) и (4) позволяют определить профиль и режимы пленочного течения. Например, при $\tau_м/\rho g\delta = 0.5$ поверхностная скорость пленки $\omega_м = 0$, но ее промежуточные слои, как следует из уравнения (3), сохраняют движение вниз.

УДК 512.624.95

Студ. И.И. Скородумов
Науч. рук. доц. Е. И. Ловенецкая
(кафедра высшей математики, БГТУ)

МАТЕМАТИЧЕСКИЕ ЗАДАЧИ АЛГОРИТМА RSA

По мере развития компьютерных сетей возникла необходимость в способе безопасного обмена конфиденциальной информацией без согласования ключей защищенными каналами связи. Благодаря этому были разработаны алгоритмы асимметричного шифрования. Одним из них является RSA[1].Они используется для создания цифровых подписей и обмена ключами симметричных шифров, т.к. шифровать сами сообщения с помощью RSA нерационально. Безопасность RSA обуславливается проблемой факторизации больших чисел (в настоящее время не существует быстрых алгоритмов разложения на простые множители больших целых чисел), а корректность шифрования следует из теоремы Эйлера о возведении в степень по модулю.

Цели работы: изучить математическое обоснование алгоритма RSA, написать свою реализацию алгоритма.

В основе алгоритма RSA лежат следующие методы и результаты теории чисел: свойства сравнений по модулю (основные действия в RSA выполняются по модулю заданного целого числа *n*); теорема Эйлера (гарантия корректности алгоритма); определение простоты больших чисел (для генерации достаточно большого *n*).

Проблемными местами безопасного использования RSA являются генерация больших простых чисел (в настоящее время исполь-

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.