Секция «Прикладная геодезия и земельный кадастр», научный руководитель – Андреева Н.В., канд. физ.-мат. наук

ОПРЕДЕЛЕНИЕ УСКОРЕНИЯ СВОБОДНОГО ПАДЕНИЯ С ПОМОЩЬЮ ОБОРОТНОГО МАЯТНИКА

Баранова Я Ю., Андреева Н.В.

БГТУ им. В.Г. Шухова, Белгород,
e-mail: baranova0895@mail.ru

Существование многочисленных гипотез о физических параметрах, размерах и геометрической форме Земли свидетельствуют, что развитие науки на нашей планете происходило поэтапно. Представление о гравитационном поле Земли постоянно менялось, в XII в. до н.э. Аристотель выдвинул гипотезу о существовании силы притяжения между Землей и другими телами.

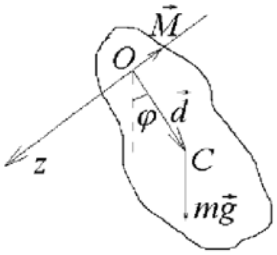
Ускорение свободного падения – g – ускорение, придаваемое телу в вакууме силой тяжести, то есть геометрической суммой гравитационного притяжения планеты (или другого астрономического тела) и сил инерции, вызванных её вращением. В соответствии со вторым законом Ньютона, ускорение свободного падения равно силе тяжести, воздействующей на объект единичной массы [1]. Экспериментально установлено, что ускорение свободного падения не зависит от массы падающего тела, но зависит от географической широты местности и высоты h подъема над земной поверхностью, что обеспечивается эллипсоидальной формой земной поверхности и ее вращением вокруг своей оси [2].

В настоящее время существует множество экспериментальных способов определения ускорения свободного падения, все они делятся на две категории: статистические и динамические методы. В статических методах тело, участвующее в измерениях, находится в момент измерения (фиксации отсчета) в покое, измеряются смещение тела или давление, вызванное весом тела. Приборы, служащие для измерения силы тяжести статическим методом, называются гравиметрами [3].

Широкое распространение получили маятниковые способы, относящиеся к динамическим методам, в которых наблюдают движение тела в гравитационном поле. Последнее представляет собой силовое поле, обусловленное притяжением масс Земли и центробежной силой, которая возникает вследствие суточного вращения планеты. Гравитационное поле характеризуется силой тяжести, потенциалом силы тяжести и различными его производными.

Маятниковые измерения – относительный метод, позволяющий определить ускорение силы тяжести между гравиметрическими пунктами. Гравиметрическими пунктами называются точки на земной поверхности, в которых измерено ускорение силы тяжести и определены плановые координаты и высоты. Сущность способа заключается в наблюдении свободных колебаний одного и того же маятника на разных пунктах. Преимуществами таких измерений являются: независимость результатов измерений, точность, независимость от продолжительности гравиметрического рейса и от сложности поля [3]. В данной статье проанализированы два способа определения ускорения свободного падения: с помощью физического и оборотного маятников.

Физический маятник – это твердое тело, совершающее под действием силы тяжести колебания вокруг неподвижной горизонтальной оси, проходящей через точку O, не совпадающую с центром масс C (рисунок).



Физический маятник

Использование произвольных физических маятников удобно для нахождения отношений значений g в различных точках поля тяготения, но при определении самого значения g возникает трудность точного определения момента инерции маятника, что исключается в методе оборотного маятника, т.к. в его расчетных формулах отсутствует величина момента инерции маятника J_0 [5].

Метод оборотного маятника основан на известном свойстве двух точек физического (точки подвеса и точки качания), при последовательном подвешивании маятника в которых его период остается неизменным. Расстояние между этими точками определяется приведенной длиной физического маятника $l_{пр}$.

Таким образом, если у физического маятника найдены две сопряженные точки, когда периоды колебаний на них T_1 и T_2 совпадают с точностью до 2-3 с (для этого необходимо выбрать такие точки на маятнике, для которых время одинакового числа колебаний будет отличаться не более чем на 0,3 с), тогда для определения g достаточно точно измерить $T_0 = T_1 = T_2$ и $l_{пр}$ равное расстоянию между этими точками [4].

Т.к. экспериментально достаточно сложно выбрать точки так, чтобы $T_1 = T_2$, то для повышения точности можно использовать теорему Штейнера, на основании которой конечная формула определения ускорения свободного падения будет выглядеть так:

$$g = \frac{4\pi^2 l_{пр}}{T_0^2},$$

где $l_{пр}$ – расстояние между выбранными точками на маятнике, а

$$T_0 = \frac{T_1 + T_2}{2} \approx T_1 \approx T_2 .$$

В ходе эксперимента при N=50, где N – количество колебаний и $l_{пр}$ = 0,230 м было проведено несколько серий измерений, по результатам которых составлена таблица.

№ п/п	$t(rc_1)$, с	$t(rc_2)$,с	$T(rc_1)$, с	$T(rc_2)$, с	g, (м/с^2)
1	47,8	47,9	0,956	0,958	9,904288
2	48,1	48,3	0,962	0,962	9,801600
Ср.	47,95	48,10	0,959	0,962	9,852944

По данным таблицы получено среднее значение ускорения свободного падения $g_{ср}$= 9,852944 м/с^2= =985244 мГал. По формуле

$$\Delta g_0 = g\left(\frac{\Delta r}{r} + \frac{2T}{T}\right)$$

была рассчитана относительная погрешность полученной величины $\Delta g_{ср}$= ±0,1125367 м/с^2=1125367 мГал. Таким образом, было установлено, что значение $g_{теор}$= 9,80665 м/с^2=980665 мГал (ускорение свободного падения на уровне моря и широте 45°), которое принято за фундаментальное, входит в доверительный интервал экспериментально полученного значения ускорения свободного падения

$$9.7404073 \text{ м/с}^2 \le g_{ср} \le 9.9654807 \text{ м/с}^2 \text{ [5].}$$

Список литературы

1. Куликов К.А. Изменяемость широт и долгот / К.А. Куликов. – М.: Гос. изд-во физико-математической литературы, 1962.

2. Перервенко Э.О., Андреева Н.В. Ускорение свободного падения на поверхности земли [Электронный ресурс]. – URL: http://www.scienceforum.ru/2014/553/1810.

3. Андреева Н.В., Баранова Я.Ю., Козлова Е.Р., Корнейчук М.А., Мартынова Н.С., Празина Е.А. Определение ускорения свободного падения маятниковым способом [Электронный ресурс] URL: http://today.science-publish.ru.

4. [Электронный ресурс]. – URL: http://physics.tsu.tula.ru/bib/lab/3/lab5-meh.pdf.

5. Андреева Н.В., Баранова Я.Ю., Козлова Е.Р., Корнейчук М.А., Мартынова Н.С., Празина Е.А. Определение ускорения свободного падения физическим маятником// Научно-исследовательский журнал European Research, 2010. – №10. – С.54.

Секция «Применение информационных технологий для повышения эффективности производства, управления, обучения», научный руководитель – Кочеткова О.В., д-р техн. наук, профессор

МАТЕМАТИЧЕСКИЙ АНАЛИЗ РОССИЙСКОГО АЛГОРИТМА ШИФРОВАНИЯ В СРАВНЕНИИ С АНАЛОГОМ – ПОБЕДИТЕЛЕМ КОНКУРСА AES

Меликов А.В., Яковлев С.Л.

Волгоградский государственный аграрный университет, Волгоград, e-mail: strizhakovaelena@mail.ru

Разработанная интеллектуальная обучающая система (ИОС) алгоритмов шифрования[1] позволяет проводить статистические исследования, примером которых является анализ «лавинного эффекта», т.е. определение зависимости каждого бита шифртекста от соответствующего бита открытого текста с учетом работы исходного ключа.

Математический анализ предлагается начать с алгоритма шифрования «Rijndael» – победителя конкурса AES [1].Предположим, что во входном 32-битовом значении изменен 1 бит. Первая операция функции шифрования – сложение по модулю 2^{32}, т.е. с переносом из младших разрядов в старшие. Теоретически, изменение самого младшего бита операнда может привести к изменению всех битов суммы. При условии равновероятного и независимого распределения битов операндов на множестве {0,1} вероятность события «влияние одного бита операнда распространяется влево ровно на *n* бит результата», равна 2^{-n}. Это означает, что если изменить значение 1 бита операнда на противоположное, то помимо соответствующего ему бита результата, который инвертируется в любом случае, ровно *n* битов результата, находящихся левее инвертированного, также поменяют значение на противоположное с указанной выше вероятностью. Получаем, что при сложении двух чисел по модулю 2^{32} практическое значение имеет только влияние бита операнда на не более, чем 4 старших бита результата.

Теперь рассмотрим диффузионные характеристики алгоритма «Rijndael». Первая операция раунда шифрования алгоритма – побитовое суммирование с ключом по модулю 2 – не приводит к выходу изменения за пределы 1 бита. Следующая операция – замена по таблице – распространяет изменение в 1 бите на весь байт. Следующий за ней построчный байтовый сдвиг не изменяет ничего. Наконец, завершающая операция раунда – перемешивание байтов в столбцах матрицы – приводит к диффузии изменения на весь столбец. Таким образом, за 1 раунд шифрования изменение в 1 бите входных данных окажет влияние на 1 столбец матрицы данных. На следующем раунде шифрования эти байты в ходе операции построчного байтового сдвига будут «разведены» по разным столбцам, и в результате последующей операции перемешивания байтов в столбцах исходное изменение распространится на 4 столбца. Диаграмма диффузии в алгоритме-финалисте конкурса AES приведена на рисунке.

Таким образом, при шифровании исходного текста изменение в одном бите входных данных распространяется на весь блок ровно за два раунда. В результате за 10-14 раундов алгоритма шифрования «Rijndael» данные успевают полностью перемешаться пять-семь раз.

Диффузия изменения в исходных данных в процессе шифрования «Rijndael»

Сформулируем основные достоинства и недостатки отечественного стандарт шифрования «ГОСТ Р 28147-89»[2]. Исходя из рассуждений Б. Шнайера [2], невосприимчивость алгоритма «ГОСТ Р 28147-89» к дифференциальному и линейному криптоанализу плюс большое количество раундов означают, что российский стандарт шифрования является достаточно надежным. К тому же, лобовое вскрытие данного алгоритма абсолютно невозможно из-за 256-битного ключа, а также возможности использования секретных значений узла замены.

При сравнении производительности алгоритмов «ГОСТ Р 28147-89» и «Rijndael» на 32-битных платформах, российский стандарт шифрования медленнее криптостандарта США, но это разница составляет всего 10-20% [3]. Преимущество алгоритма AES невелико, потому что отечественный криптостандарт

[1]Яковлев, С.Л. Разработка интеллектуальной обучающей системы современных алгоритмов шифрования: Магистерская диссертация / под науч. рук. доц. А.В. Меликова. – Волгоград: ВолГАУ, 2015. – 101 с.

[2]ГОСТ 28147-89. Группа П85. Государственный стандарт союза СССР. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. ОКП 40 4000.Дата введения 1990-07-01.