УДК 378.147.1:004.9

ИНТЕНСИФИКАЦИЯ УЧЕБНОГО ПРОЦЕССА С ИСПОЛЬЗОВАНИЕМ MAPLE

© Литвинов А.Л.
Украинская инженерно-педагогическая академия

Інформація про автора:
Литвинов Анатолій Леонідович: «Інтенсифікації учбового процесу з використанням Maple» ; ORCID: 0000-0001-7063-7814; litan@meta.ua; доктор технічних наук, професор, завідуючий кафедрою радіоелектроніки і комп'ютерних систем; Українська інженерно-педагогічна академія; вул. Університетська, 16, м. Харків, 61003, Україна.

У статті представлені результати використання системи комп'ютерної математики Maple для складання завдань для контрольних робіт, для контролю процесу виконування практичних робіт, пояснення завдань позамежній складності і створення віртуальних лабораторій. Використовувані на різних етапах навчання, ці методи показали ефективність системи Maple, як необхідного елементу учбового процесу, використання якого дозволяє підвищити його ефективність.

Ключові слова: Maple, складання завдань, контроль, практичні робити, криптографія, секретний ключ, просте число, віртуальна лабораторія, перехідний процес.

Литвинов А.Л. «Интенсификация учебного процесса с использованием Maple»
В статье представлены результаты использования системы компьютерной математики Maple для составления заданий для контрольных работ, для контроля процесса выполнения практических работ, объяснения задач запредельной сложности и создания виртуальных лабораторий. Используемые на разных этапах обучения, эти методы показали эффективность системы Maple, как необходимого элемента учебного процесса, использование которого позволяет повысить его эффективность.

Ключевые слова: Maple, составление заданий, контроль, практические работы, криптография, секретный ключ, простое число, виртуальная лаборатория, переходной процесс.

A. Litvinov **«**Intensification of educational process using Maple»
The article presents the results of the use of computer mathematics Maple to compose tasks for control works, for monitor of the implementation of practical work, explaining problems prohibitive complexity and create virtual laboratories. Used at various stages of training, these methods have shown the effectiveness of Maple, as a necessary element of the educational process, the use of which can improve its effectiveness.

Keywords: Maple, compose tasks, monitor, practical work, secret key, prime number, virtual laboratory, transitional process.

Постановка проблемы. В науке и технике широко используется система компьютерной математики (СКМ) Maple, ориентированная на аналитическое и численное решение математических задач. Maple имеет мощный встроенный язык программирования, аналогичный Паскалю. Количество встроенных функций, которые охватывают все разделы математики и смежных дисциплин доходит до 5000, что сводит программирование при решении практических задач до минимума. Система Maple реализована в среде операционной системы Windows и имеет совместимый с ней интерфейс, что упрощает работу с ней. СКМ Maple имеет прекрасно выполненную справочную систему с большим количеством примеров, что значительно облегчает решение конкретных задач. Для практически любой математической задачи в справочной системе можно найти аналог и после небольших доработок использовать его. Следует отметить, что в большинстве случаев СКМ Maple используется для целей анализа. В связи с этим формулируется проблема расширения областей применения СКМ Maple, например: для составления заданий по математике, для контроля хода решения задач, как виртуальную лабораторию.

Анализ последних исследований и публикаций. С момента своего появления СКМ Maple привлекла исследователей своей функциональной завершенностью, широкими возможностями, легкостью освоения [1, 2]. Описание системы Maple, основные приемы работы с ней приведены в фундаментальных работах Дьяконова В.П. [3, 4]. Использование системы Maple для решения задач теории графов приведено в [5] . Особенностью СКМ Maple является наличие специализированных пакетов, ориентированных на конкретные области применения. Применению Maple для моделирования технико-экономических систем посвящены работы [6, 7]. В работе Попова Б.А. [9] приведены как основы работы с системой Maple, так приемы решению математических задач в ней. Таким образом СКМ Maple широко используется в различных областях исследований, но с ориентацией на решение задач анализа. Применению Maple в учебном процессе уделяется недостаточное внимание.

Постановка задач исследования. Целью статьи является обобщение опыта автора по использованию СКМ Maple в учебном процессе. Обладая уникальными свойствами по аналитическим преобразованиям, СКМ Maple позволяет облегчить труд преподавателя по составлению заданий, контролю правильности хода вычислений. СКМ Maple позволяет визуализировать результаты вычислений в 2D и 3D форматах, что позволяет студентам четко понять суть происходящих процессов.

Изложение основного материала исследования. Одной из актуальных задач для преподавателя является обновление заданий для контрольных работ, выполняемых студентами самостоятельно. В общем, задача весьма трудоемкая, так как ее надо составить так, чтобы студент получил ясный результат. Использование системы Maple позволяет существенно снизить нагрузку на преподавателя и повысить эффективность его работы. Приведем соответствующие примеры.

В математике широко используется операция разложения неправильной дробно-рациональных функций на простейшие дроби. Как промежуточная, но важная, эта операция выполняется при интегрировании дробно-рациональных функций, при вычислении оригинала по изображению в преобразовании Лапласа. Сама по себе эта операция весьма трудоемкая. Произвольно выбранная дробь может не иметь «удобного для студента» разложения. Решим эту задачу в Maple.

а. Задаем конечное выражение, содержащее целую часть и простейшие дроби, например

$$r := x+9+\frac{4}{x-5}+\frac{6}{x^2+2x+8}. \qquad (1)$$

б. С помощью команды combine(r, trig) преобразуем выражение для r в неправильную дробно-рациональную функцию.

$$r=\frac{x^4+6x^3-25x^2-44x-358}{x^3-3x^2-2x-40}. \qquad (2)$$

В таком виде задание будет выдаваться студенту для разложения на простейшие дроби, а именно вида (1). Главное, преподаватель знает ответ без необходимости самостоятельно решать все варианты. Меняя параметры в выражении (1) можно легко составлять новые задания.

Особенно эффективно применение Maple, когда необходимо контролировать преобразования по отдельным этапам. Рассмотрим следующую задачу финансовой математики.

Создан фонд стоимостью P грн. Спустя n_1 лет его стоимость составила $S(n_1)$ грн., а спустя n_2 лет его стоимость составила $S(n_2)$ грн. Определить стоимость фонда спустя n_3 лет, если его наращение осуществляется по непрерывной ставке с силой роста, изменяющейся по линейному закону $\delta(t)=\delta_0+at$. Выполнить контроль правильности расчетов. Расчеты вести с точностью до четырех значащих цифр. Исходные данные представлены в табл.1.

Таблица 1

Исходные данные для расчета стоимости фонда

Номер варианта	P (тысяч грн)	n_1 (года)	$S(n_1)$ (тысяч грн)	n_2 (года)	$S(n_2)$ (тысяч грн)	n_3 (года)
1	85	2,5	101	3,5	134	4,8
2	23	1,8	36	2,9	45	4,1
3	60	1,9	84	2,8	103	3,7
4	30	2,7	43	3,6	51	5,1
5	71	2,1	92	2,9	102	4,1.
6	75	1,7	88	2,1	98	3,7
7	25	2,4	36	3,7	45	5,2

Для расчетов используются следующие формулы:

При наращении по непрерывной ставке с силой роста, изменяющейся по линейному закону, наращенная сумма вычисляется по формуле [10]

$$S(n)=Pe^{\delta_0 n+\frac{an^2}{2}}=P\cdot\exp\left(\delta_0 n+\frac{an^2}{2}\right). \tag{3}$$

Подставив в выражение (3) данные, соответствующие времени n_1, получим линейное уравнение

$$S(n_1)=P\cdot\exp\left(\delta_0 n_1+\frac{an_1^2}{2}\right)\Rightarrow\ln\left(\frac{S(n_1)}{P}\right)=n_1\delta_0+\frac{n_1^2}{2}a\,. \tag{4}$$

Подставив в выражение (3) данные, соответствующие времени n_2, получим линейное уравнение

$$S(n_2)=P\cdot\exp\left(\delta_0 n_2+\frac{an_2^2}{2}\right)\Rightarrow\ln\left(\frac{S(n_2)}{P}\right)=n_2\delta_0+\frac{n_2^2}{2}a\,. \tag{5}$$

Таким образом, получили систему линейных уравнений второго порядка относительно δ_0 и a:

$$n_1\delta_0+\frac{n_1^2}{2}a=\ln\left(\frac{S(n_1)}{2}\right),\quad n_2\delta_0+\frac{n_2^2}{2}a=\ln\left(\frac{S(n_2)}{2}\right). \tag{6}$$

Таким образом, получили систему линейных уравнений второго порядка относительно δ_0 и a:

$$n_1\delta_0+\frac{n_1^2}{2}a=\ln\left(\frac{S(n_1)}{2}\right),\quad n_2\delta_0+\frac{n_2^2}{2}a=\ln\left(\frac{S(n_2)}{2}\right). \tag{6}$$

Решив систему уравнений (6) относительно δ_0 и a, получим конкретное выражение для формулы наращения стоимости фонда. Теперь можно найти стоимость фонда в момент n_3 лет после его создания.

Пример. $P = 142$ тыс. грн., $n_1 = 2,2$ лет, $n_2 = 3,4$ года. После соответствующих преобразований система линейных уравнений второго порядка относительно δ_0 и a будет иметь вид:

$$\begin{aligned} 2,2\delta_0 + 2,42a &= 0,137923\,, \\ 3,4\delta_0 + 5,78a &= 0,342490. \end{aligned} \qquad (7)$$

Решив ее по формулам Крамера, получим

$$\delta_0 = \text{-}0.0070478, \quad \mathrm{a} = 0.063400\,.$$

Выражение для формулы наращения стоимости фонда имеет вид:

$$S(n) = 142000e^{-0.0070478\mathrm{n}+\frac{0.063400\mathrm{n}^2}{2}}\,.$$

Контроль правильности расчетов. Подставим в формулу для наращенной суммы $n = 2,2$, получим:

$$S(2,2) = 142000e^{\text{-}0.0070478\cdot 2,2+0.063400\cdot 2,2^2/2} = 162999,95 \approx 163000.$$

Аналогично

$$S(3,4) = 142000e^{\text{-}0.0070478\cdot 3,4+0.063400\cdot 3,4^2/2} = 199999,97 \approx 200000,$$

что совпадает с данными в постановке задачи.

Найдем стоимость фонда в момент $n_3 = 4,5$ лет после его создания.

$$S(4,5) = 142000e^{\text{-}0.0070478\cdot 4,5+0.063400\cdot 4,5^2/2} = 261396 \text{ (руб.)}$$

Расчеты оформим в виде таблицы Maple. В отличие от табличных процессоров типа Excel, в ячейки таблицы Maple можно заносить числа, матрицы, выражения для работы с матрицами и решения уравнений разного вида.

На рис. 1 представлен фрагмент таблицы Maple для расчета наращенной суммы при конкретных значениях исходных данных.

	A	B	C	D	E	F	G	H	I	J	K
1	*Вар*	"P"	*n1*	"S1"	*n2*	"S2"	*n3*	*A*	*B*	$\begin{bmatrix} \text{"delta·0"} \\ \text{"a"} \end{bmatrix}$	*S3*
2	*Прим*	142.	2.2	163.	3.4	200.	4.5	$\begin{bmatrix} 2.200 & 2.420 \\ 3.400 & 5.780 \end{bmatrix}$	$\begin{bmatrix} 0.1379 \\ 0.3425 \end{bmatrix}$	$\begin{bmatrix} -0.0070479 \\ 0.0634000 \end{bmatrix}$	261396.
3	1	85.	2.5	101.	3.5	134.	4.8	$\begin{bmatrix} 2.500 & 3.125 \\ 3.500 & 6.125 \end{bmatrix}$	$\begin{bmatrix} 0.1725 \\ 0.4552 \end{bmatrix}$	$\begin{bmatrix} -0.0836777 \\ 0.1221323 \end{bmatrix}$	232284.
4	2	23.	1.8	36.	2.9	45.	4.1	$\begin{bmatrix} 1.800 & 1.620 \\ 2.900 & 4.205 \end{bmatrix}$	$\begin{bmatrix} 0.4480 \\ 0.6712 \end{bmatrix}$	$\begin{bmatrix} 0.2774822 \\ -0.0317551 \end{bmatrix}$	54942.
5	3	60.	1.9	84.	2.8	103.	3.7	$\begin{bmatrix} 1.900 & 1.805 \\ 2.800 & 3.920 \end{bmatrix}$	$\begin{bmatrix} 0.3365 \\ 0.5404 \end{bmatrix}$	$\begin{bmatrix} 0.1435160 \\ 0.0353417 \end{bmatrix}$	129965.
6	4	30.	2.7	43.	3.6	51.	5.1	$\begin{bmatrix} 2.700 & 3.645 \\ 3.600 & 6.480 \end{bmatrix}$	$\begin{bmatrix} 0.3600 \\ 0.5306 \end{bmatrix}$	$\begin{bmatrix} 0.0911472 \\ 0.0312498 \end{bmatrix}$	71697.

Рис. 1. Фрагмент таблицы Maple для расчета наращенной суммы

В ячейки столбца ***H*** заносятся выражения для расчета матриц системы (6) по исходным данным каждого варианта:

array(1 .. 2,1 .. 2,[[~C2, ~C2^2/2], [~E2, ~E2^2/2]]),

В ячейки столбца ***I*** заносятся выражения для расчета свободных членов системы (6) по исходным данным каждого варианта:

array(1 .. 2,1 .. 1,[[ln(~D2/~B2)], [ln(~F2/~B2)]])

В ячейки столбца ***J*** заносятся выражения для решения системы уравнений (6) по исходным данным каждого варианта матричным способом:

~H2^(-1)*~I2

В ячейки столбца ***K*** заносятся выражения для расчета стоимость фонда в момент n_3 лет после его создания

~B2*exp(~J2[1,1]*~G2+~J2[2,1]*~G2^2/2)*1000

Таким образом можно проконтролировать все этапы расчетов по каждому варианту.

Способность системы Maple работать с целыми числами огромного порядка позволяет студентам активно усваивать сложнейшие алгоритмы криптографии. Наиболее сложными являются алгоритмы с открытыми ключами; они позволяют путем обмена открытой информацией сформировать общий секретный ключ или произвести одностороннее шифрование передаваемой информации [8].

Рассмотрим, как производится формирование общего секретного ключа. В основу положены элементы теории сравнений [8]. Это так называемая схема Диффи-Хеллмана.

Отправитель и Получатель договариваются о двух достаточно больших чисел a и m. m должно быть простым. Отправитель вырабатывает случайное простое секретное число x, $1 < x < m$, вычисляет $L_i \equiv a^x \mod m$ - остаток от деления числа a^x на m и посылает L_i Получателю.

Получив L_i, Получатель вырабатывает случайное простое секретное число $y,\ 1<y<m$, вычисляет $L_j \equiv a^y \bmod m$ - остаток от деления числа a^y на m и посылает L_j Отправителю. После вычисляет $k_j = L_i^y \bmod m$.

Рассмотрим алгебраические операции при прохождении информации от отправителя к получателю.

Выражение $L_i \equiv a^x \bmod m$ означает, что $a^x - L_i$ делится нацело на m, то есть $\frac{a^x - L_i}{m} = r_i$, где r_i какое-то целое число. Тогда $L_i = a^x - r_i \cdot m$.

Операция $k_j = L_i^y \bmod m$ означает, что $L_i^y - k_j$ делится нацело на m, пусть это будет целое s_j, то есть

$$\frac{L_i^y - k_j}{m} = s_j \Rightarrow \frac{(a^x - r_i \cdot m)^y - k_j}{m} = s_j. \qquad (8)$$

Откуда

$$(a^x - r_i \cdot m)^y - k_j = s_j \cdot m \Rightarrow a^{xy} + \sum_{e=1}^{y} (-1)^e \binom{y}{e} a^{x(y-e)} (r_i \cdot m)^e - k_j = s_j \cdot m. \qquad (9)$$

Из (9) следует, что

$$a^{xy} - k_j = s_j \cdot m - \sum_{e=1}^{y} (-1)^e \binom{y}{e} a^{x(y-e)} (r_i \cdot m)^e. \qquad (10)$$

Правая часть выражения (10) делится нацело на m. Следовательно и левая часть выражения (10) делится нацело на m. А это означает, что

$$k_j \equiv a^{xy} \bmod m. \qquad (11)$$

Отправитель, получив L_j, вычисляет $k_i \equiv L_j^x \bmod m$. Повторив вышеприведенные выкладки для $k_i \equiv L_j^x \bmod m$, получим

$$k_i \equiv a^{yx} \bmod m = k_j \equiv a^{xy} \bmod m = k. \qquad (12)$$

Общий секретный ключ k сформирован. Противник, перехватив L_i или L_j при соответствующем выборе чисел a и m, не сможет за обозримое время путем перебора найти x или y и взломать рассчитать секретный ключ k. Пример формирования секретного ключа по схеме Диффи-Хеллмана приведен в табл.2.

Таблица 2

Пример формирования секретного ключа по схеме Диффи-Хеллмана.

Отправитель	Получатель
Пусть $a = 79,\ m = 489133282872437279$	
$x = 524287$ $L_i = a^x \bmod m = 432343903510583740$ →	$L_i = 432343903510583740$ $y = 936919$

L_j = *383499009556930374* $K_i = L_j^x \, mod \, m$ = *36907353303338278*	$L_j = a^y \, mod \, m$ = *383499009556930374* $K_j = L_i^x \, mod \, m$ = *36907353303338278*
$K_i = K_j = K$ = *36907353303338278* – общий секретный ключ сформирован	

Чтобы противнику заполучить секретный ключ, например по перехваченному значению L_i, можно перебрать всевозможные значения:

$P_i = a^s \, mod \, m$ по s от 1 до m= *489133282872437279* .

По идее, если найдено s, при котором $P_i = L_i$, то это и будет искомое x . А по x нетрудно найти общий секретный ключ. При проведении вычислительного эксперимента с приведенными исходными данными в системе Maple на достаточно мощном компьютере в течение длительного времени, искомое x не было найдено, а счет пришлось принудительно прервать. Кроме того, при меньших значения a, m, x, y , оказалось, что одинаковые остатки L_i получаются при разных значениях s , что еще более усложняет задачу взлома секретного ключа.

Если имеется математическое описание процессов, происходящих в электрических цепях, а нет соответствующего оборудования для их изучения, то Maple может использоваться как виртуальная лаборатория.

На рис. 2 представлен процесс синтеза периодического процесса из прямоугольных импульсов рядом Фурье из ограниченного числа гармоник. Отчетливо видно возникновение эффекта Гиббса, волнообразных колебаний на вершинах и впадинах импульсов, которые нарастают к моментам перехода от минимума к максимуму и наоборот.

```
n:=50:F:=proc(t)
0.5+sum((2/(2*k-1)/Pi)*sin((2*k-1)*t/2.115*Pi),k=1..n)
end:
plot(F,-6.7..6.7,-0.05..1.1,color=black,labels=["t","F"]);
```

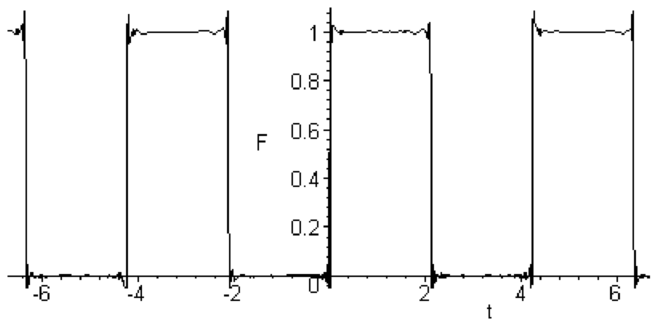


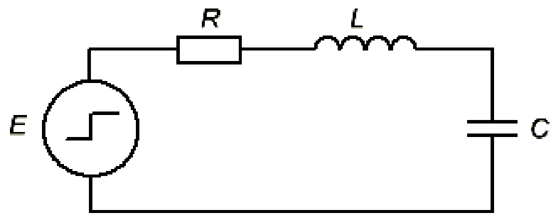
Рис.2. Моделирование периодического процесса рядом Фурье

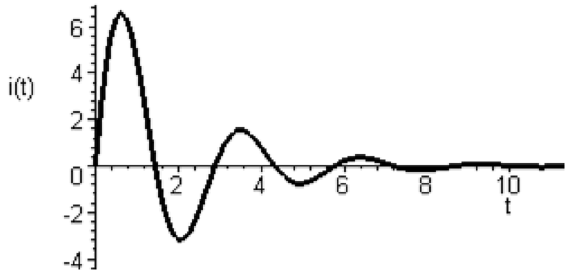
На рис. 3 представлен график затухающего колебательного процесса в последовательном RLC контуре при действии перепада напряжения. Выражение для тока получено в результате решения в системе Maple дифференциального уравнения второго порядка

$$L\frac{d^2 i}{dt}+R\frac{di}{dt}+\frac{1}{c}i=0$$

с начальными условиями

$$i(0)=0,\ i'(0)=\frac{E}{L}$$





а б

Рис. 3. Вид переходного процесса в RLC контуре: а – схема RLC контура; б – график затухающего колебательного процесса $i := t \to 9.17662 \cdot e^{(-0.500000\,t)} \sin(2.17945 \cdot t)$

Меняя параметры, например сопротивления, можно проследить изменение вида переходного процесса.

Выводы. Система компьютерной математики Maple должна стать составным элементом учебного процесса, особенно в технических ВУЗах. С ее помощью можно организовать контроль учебного процесса, выполнять преобразования, доступные майнфреймам, а также использоваться в качестве виртуальной лаборатории.

Перспективы дальнейших исследований. Проведенные исследования охватывают только небольшую часть возможностей СКМ Maple. Весьма перспективным является направление, по созданию автоматизированных систем контроля знаний, созданию виртуальных лабораторий в разных областях техники. Эти задачи можно решить с помощью так называемых маплетов – встроенных средств автоматизации вычислений с возможностью визуального диалога оператора с системой.

Список використаних джерел

1. Алексеев Е. Р. Решение задач вычислительной математики в пакетах Mathcad 12, MATLAB 7, Maple 9 / Е. Р. Алексеев, О. В. Чеснокова. – М.: НТ Пресс, 2006. – 496 с. – (Самоучитель).

2. Голоскоков Д. П. Уравнения математической физики. Решение задач в системе Maple / Д. П. Голоскоков. – М.: Питер, 2004. – 544 с.

3. Дьяконов В. П. Maple 8 в математике, физике и образовании / В. П. Дьяконов. – М.: СОЛОН-Пресс, 2003. – 656 с.

4.Дьяконов, В. П. Maple 10/11/12/13/14 в математических расчетах / В. П. Дьяконов. – М.: ДМК-Пресс, 2011. – 800 с.

5. Литвинов А. Л. Компьютерное моделирование в экономике : учеб. пособие / А. Л. Литвинов. – Белгород: Изд-во БелГУ, 2004. – 108 с.

6. Литвинов А. Л. Математичні методи та моделі в розрахунках на ЕОМ. Система Maple та її використання для моделювання техніко-економічних систем : навч. посіб. для спец. "Теплові електричні станції", а також для магістрів і аспірантів / А. Л. Литвинов ; Укр. інж.-пед. акад. – Харків : [б. в.], 2004. – 103 с.

7. Попов Б. О. Розв’язання математичних задач у системі комп’ютерної алгебри Maple V / Б.О. Попов. – Київ: VIP, 2007. – 312 с.

8. Четыркин Е. М. Финансовая математика: учебник / Е. М. Четыркин. – М.: Дело, 2004. – 400 с

9. Кирсанов М. Н. Графы в Maple / М. Н. Кирсанов. – М.: Физматлит, 2007. – 168 с.http://vuz.exponenta.ru/PDF/book/GrMaple.pdf

10. Венбо Мао. Современная криптография: теория и практика / Мао Венбо ; пер. с англ. – М.: Вильямс, 2005. – 768 с.

Referenses

1. Alekseyev, YeR & Chesnokova, OV 2006, *Resheniye zadach vychislitelnoi matematiki v paketakh Mathcad 12, MATLAB 7, Maple 9*, NT Press, Moskva.

2. Goloskokov, DP 2004, *Uravneniya matematicheskoy fiziki. Resheniye zadach v sisteme Maple*, Piter, Moskva.

3. Dyakonov, VP 2003, *Maple 8 v matematike, fizike i obrazovanii*, SOLON-Press, Moskva.

4. Dyakonov, VP 2011, *Maple 10/11/12/13/14 v matematicheskikh raschetakh*, DMK-Press, Moskva.

5. Litvinov, AL 2004, *Kompyuternoye modelirovaniye v ekonomike,* Izdatelstvo Belgorodskogo gosudarstvennogo univeresiteta, Belgorod.

6. Litvinov, AL 2004, *Matematichni metody ta modeli v rozrakhunkakh na EOM. Sistema Maple ta її vykorystannia dlia modeliuvannia tekhniko-ekonomichnykh system*, Kharkiv.

7. Popov, BO 2007, *Rozviazannia matematichnikh zadach u sistemi komiyuternoi algebry Maple V*, VIP, Kyiv.

8. Chetyrkin, EM 2004, *Finansovaya matematika*, Delo, Moskva.

9. Kirsanov, MN 2007, *Grafy v Maple,* Fizmatlit, Moskva.

11. Venbo, Mao 2005, *Sovremennaya kriptografiya: teoriya i praktika*, [*Modern Cryptography: Theory and Practice*]**,** Vilyams, Moskva.

Стаття надійшла до редакції 16.04.2015р.