7. Park, J. Towards usage control models: beyond traditional access control [Text] / J. Park, R. Sandhu // Proceedings of the seventh ACM symposium on Access control models and technologies SACMAT 02. — 2002. — P. 57—64.
8. Kulkarni, D. Context-aware role-based access control in pervasive computing systems [Text] / D. Kulkarni, A. Tripathi // Proc. 13th ACM Symp. Access Control Model. Technol. SACMAT 08. — 2008. — P. 113.
9. Priebe, T. Supporting Attribute-based Access Control in Authorization and Authentication Infrastructures with Ontologies [Text] / T. Priebe, W. Dobmeier, C. Schläger, N. Kamprath // J. Software. — 2007. — Vol. 2, no. 1. — P. 27—38.
10. Thomas, R. K. Conceptual Foundations for a Model of Task-based Authorizations [Text] / R. K. Thomas, R. S. Sandhu // Proceedings of the 7th IEEE Computer Security Foundations Workshop. — 1994. — Vol. 39, no. 1. — P. 66—79.

УПРАВЛЕНИЕ ДОСТУПОМ К РЕСУРСАМ ИНТЕЛЛЕКТУАЛЬНОГО ПРЕДПРИЯТИЯ С ИСПОЛЬЗОВАНИЕМ ОНТОЛОГИЧЕСКИХ МОДЕЛЕЙ

Предложено подход для управления доступом к ресурсам интеллектуального предприятия, который использует онтологические модели. По сравнению с известными методами RBAC и ABAC, предложенный метод создает возможность динамического, документированного присвоения и изъятия прав доступа к ресурсам в контексте бизнес-процессов, которые выполняются в системе.

Ключевые слова: управление доступом, онтологическая модель, моделирование бизнес-процессов, интеллектуальная система, интеллектуальное предприятие.

Буров Євген Вікторович, *кандидат технічних наук, доцент, професор кафедри інформаційних систем та мереж, Національний університет «Львівська політехніка», Україна,*
e-mail: eugeneburov01@gmail.com*.*

Буров Евгений Викторович, *кандидат технических наук, доцент, профессор кафедры информационных систем и сетей, Национальный университет «Львовская политехника», Украина.*

Burov Yevhen, *National University «Lviv Polytechnic», Ukraine,*
e-mail: eugeneburov01@gmail.com

УДК 378.14+004.4

Литвинов А. Л.

АКТИВНЫЕ МЕТОДЫ ОБУЧЕНИЯ В СИСТЕМЕ КОМПЬЮТЕРНОЙ МАТЕМАТИКИ MAPLE

Представлены результаты использования системы компьютерной математики Maple для контроля знаний, 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, контроль знаний, криптография, секретный ключ, простое число, виртуальная лаборатория, эффект Гиббса, процесс.*

1. Введение

Системы компьютерной математики Mathcad, Matlab, Maple заняли прочное место при проведении научных расчетов, в анализе экспериментальных данных [1]. Особое место среди них занимает система Maple, ориентированная как на символьные, так и численные вычисления [2, 3]. В настоящее время в учебном процессе система Maple в основном используется как естественная замена системам программирования за счет огромного числа встроенных функций и процедур [4, 5]. В тоже время возможности системы Maple выходят за рамки традиционных подходов и позволяют ее использовать как активное средство обучения, позволяющее повысить качество обучения.

2. Контроль знаний с помощью системы Maple

Преподаватели тратят массу времени на составление и проверку студенческих домашних заданий. Использование системы Maple позволяет существенно снизить их нагрузку. 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 $\delta(t)=\delta_0+at$. Наращенная сумма вычисляется по формуле [6]:

$$S(n)=P\cdot\exp\left(\delta_0 n+\frac{an^2}{2}\right). \quad (1)$$

Подставив в выражение (1) данные, соответствующие времени n_1 и n_2, после соответствующих преобразований, получим систему линейных уравнений второго порядка относительно δ_0 и a:

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

Решив систему уравнений (2) относительно δ_0 и a матричным способом, можно найти стоимость фонда в момент n_3 лет после его создания. 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*	"delta 0" "a"	*S3*
2	1	85.	2.5	101.	3.5	134.	4.8	2.500 3.125 / 3.500 6.125	0.1725 / 0.4552	-0.0836777 / 0.1221323	232284.
3	2	23.	1.8	36.	2.9	45.	4.1	1.800 1.620 / 2.900 4.205	0.4480 / 0.6712	0.2774822 / -0.0317551	54942.

Рис. 1. Фрагмент таблицы Maple для расчета наращенной суммы

По исходным данным для каждого варианта в ячейки столбцов *H*, *I* и *J* заносятся выражения для расчета матрицы системы (2), свободных членов и решения системы уравнений (2) матричным способом. Соответственно,

array(1 .. 2,1 .. 2,[[~C2, ~C2^2/2], [~E2, ~E2^2/2]]),
array(1 .. 2,1 .. 1,[[ln(~D2/~B2)], [ln(~F2/~B2)]]),
~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.

Таблица на рис. 1 позволяет проконтролировать все этапы расчетов по каждому варианту.

3. Использование Maple в криптографии

Способность системы Maple работать с целыми числами огромного порядка позволяет студентам активно усваивать сложнейшие алгоритмы криптографии, которые обычно реализуются на мэйнфреймах. Наиболее сложными являются алгоритмы с открытыми ключами; они позволяют путем обмена открытой информацией сформировать общий секретный ключ или произвести одностороннее шифрование передаваемой информации [7, 8].

Рассмотрим, как производится формирование общего секретного ключи. В основу положены элементы теории сравнений [9, 10]. Это так называемая схема Диффи-Хелмана (табл. 1).

Таблица 1

Пример схемы Диффи-Хелмана

Отправитель	Получатель
Пусть $a = 79$, $m = 489133282872437279$	
$x = 524287$	
$L_i = a^x \bmod m = 432343903510583740$ →	$L_i = 432343903510583740$
	$y = 936919$
$L_j = 383499009556930374$ ←	$L_j = a^y \bmod m = 383499009556930374$
$K_i = L_j^x \bmod m = 36907353303338278$	$K_j = L_i^x \bmod m = 36907353303338278$
$K_i = K_j = K = 36907353303338278$ — общий секретный ключ сформирован	

Отправитель и Получатель договариваются о двух достаточно больших числах a и m. m должно быть простым. Отправитель вырабатывает случайное простое секретное число x, $1 < x < m$, вычисляет $L_i \equiv a^x \bmod m$ — 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 этого вычисляет $k_j = L_i^y \bmod m$. Отправитель, получив L_j, вычисляет $k_i \equiv L_j^x \bmod m$. k_i и k_j совпадают. Таким образом, выработан общий секретный ключ k. 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 секретный ключ k.

Чтобы противнику заполучить секретный ключ, например по перехваченному значению L_i, необходимо перебрать всевозможные значения $P_i = a^s \bmod m$ по s от 1 до $m = 489133282872437279$, а это нереально.

4. Использование Maple как виртуальной лаборатории

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.

```
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"]);
```

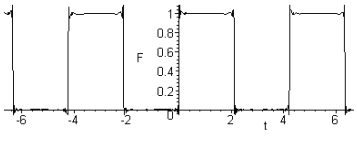


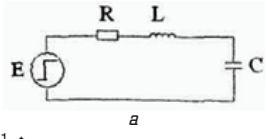
Рис. 2. Моделирование периодического процесса рядом Фурье

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:

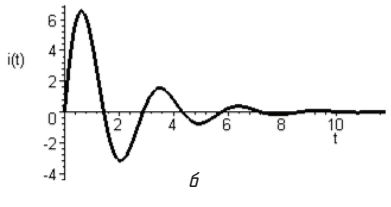
$$L\frac{d^2i}{dt} + R\frac{di}{dt} + \frac{1}{c}i = 0$$

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

$$i := t \to 9.17662 \cdot e^{(-0.500000t)} \sin(2.17945 \cdot t)$$

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

5. 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.

Литература

1. Алексеев, Е. Р. Решение задач вычислительной математики в пакетах Mathcad 12, MATLAB 7, Maple 9 [Текст] / Е. Р. Алексеев, О. В. Чеснокова. — М.: НТ Пресс, 2006. — 496 с.
2. Говорухин, В. Н. Введение в Maple. Математический пакет для всех [Текст] / В. Н. Говорухин, В. Г. Цибулин. — М.: Мир, 1997. — 208 с.
3. Дьяконов, В. П. Maple 10/11/12/13/14 в математических расчетах [Текст] / В. П. Дьяконов. — М.: ДМК-Пресс, 2011. — 800 с.
4. Литвинов, А. Л. Компьютерное моделирование в экономике [Текст] : учеб. пособ. / А. Л. Литвинов. — Белгород: Изд-во БелГУ, 2004. — 108 с.
5. Литвинов, А. Л. Математичні методи та моделі в розрахунках на ЕОМ. Система Maple та її використання для моделювання техніко-економічних систем [Текст] : навч. посіб. / А. Л. Литвинов. — Харків: УІПА, 2004. — 103 с.
6. Четыркин, Е. М. Финансовая математика [Текст] : учебник / Е. М. Четыркин. — М.: Дело, 2004. — 400 с.
7. Баричев, С. Г. Основы современной криптографии [Текст] / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. — М.: Горячая линия — Телеком, 2002. — 175 с.
8. Венбо Мао. Современная криптография: теория и практика [Текст] / Мао Венбо. — М.: Издательский дом «Вильяме», 2005. — 768 с.
9. Оре, О. Приглашение в теорию чисел [Текст] / О. Оре. — М.: Наука, 1980. — 128 с.
10. Бондарев, В. М. Основы программирования [Текст] / В. М. Бондарев, В. И. Рублинецкий, Е. Г. Качко. — Харьков: Фолио, 1997. — 368 с.

АКТИВНІ МЕТОДИ НАВЧАННЯ У СИСТЕМІ КОМП'ЮТЕРНОЇ МАТЕМАТИКИ MAPLE

Представлені результати використання системи комп'ютерної математики Maple для контролю знань, пояснення завдань позамежної 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, контроль знань, криптографія, секретний ключ, просте число, віртуальна лабораторія, ефект Гіббса, процес.

Литвинов Анатолий Леонидович, *доктор технических наук, профессор, заведующий кафедрой радиоэлектроники и компьютерных систем, Украинская инженерно-педагогическая академия, Харьков, Украина,* ***e-mail: litan@meta.ua****.*

Литвинов Анатолій Леонідович, *доктор технічних наук, професор, завідуючий кафедри радіоелектроніки і комп'ютерних систем, Українська інженерно-педагогічна академія, Харків, Україна.*

Litvinov Anatoliy, *Ukrainian Engineering Pedagogics Academy, Kharkiv, Ukraine,* ***e-mail: litan@meta.ua***

УДК 316.6+159.923

Соколова І. М., Нікітіна О. П.

ПЕРЕДУМОВИ СОЦІАЛЬНО-ПСИХОЛОГІЧНОЇ АДАПТАЦІЇ СТУДЕНТІВ-ТУРКМЕН, ЯКІ НАВЧАЮТЬСЯ В УКРАЇНІ

Представлено результати дослідження передумов соціально-психологічної адаптації студентів-туркмен, які навчаються в українських вищих навчальних закладах. Особливості ставлення до Іншого визначено як важливу передумову соціально-психологічної адаптації іноземних студентів. Виявлено взаємозв'язки показників соціально-психологічної адаптації з показниками вираження різних стилів міжособистісної взаємодії у студентів-туркмен.

Ключові слова: *соціально-психологічна адаптація, міжособистісна взаємодія, навчання іноземних студентів, студент-туркмен.*

1. Вступ та актуальність роботи

Перед українським ВНЗ стоїть першочергове завдання оптимізувати життя та навчання іноземних студентів, які проходять через складний процес адаптації до нових умов їх життєдіяльності. Успішна адаптація сприяє, з одного боку, швидкому включенню студентів у навчальний процес, що дозволяє вирішувати проблему збереження контингенту учнів, який істотно скорочується під час перших сесій, а з іншого — допомагає підвищити якість підготовки молодих людей в українських ВНЗ.

2. Аналіз літературних даних і постановка проблеми

Соціально-психологічна адаптація визначається як результат (і процес) взаємодії особистості та соціального середовища; передбачає активне прийняття і засвоєння особистістю норм, цінностей, традицій колективу, статусу та соціальної ролі, як члена колективу, оточення; дозволяє індивідууму задовольняти актуальні потреби і реалізовувати пов'язані з ними значущі цілі, забезпечуючи в той же час відповідність діяльності людини, її поведінки вимогам середовища [1].