одновременно вычисляется $H(T)=m'$ по расшифрованному тексту T. При совпадении m и m' цифровая подпись считается подлинной и ее владелец может нести ответственность за текст или допускается к входу в названный узел сети.

При использовании операции гаммирования передающая и принимающая информацию стороны могут иметь идентичную таблицу случайных чисел. Секретность гаммирования может обеспечиваться путем зашифрованного начального случайного числа в таблице, либо оно может вычисляться по известной пользователям функции, содержащей среди переменных время передачи текста.

Учитывая, что при шифровании работа ведется с двоичными кодами и основой для операции гаммирования является последовательность из нулей и единиц, отметим как результаты чтения таблицы случайных чисел перевести в удобную для приложений форму. Для этой цели можно читать таблицу случайных чисел по строкам, преобразуя каждую десятичную цифру в двоично-десятичный код. При порождении последовательности из нужного количества двоичных знаков она складывается с полученным текстом Т поразрядно по модулю 2 (1 + 1 = 0, 0 + 1 = 1) и получаем зашифрованный текст который подготовлен в точке отправления. Так как он вычислен по одним и тем же законам в пункте оправления и получения текста Т на одинаковом отрезке случайной последовательности благодаря общей исходной таблице, распространяемой операции пользователей сети.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Конышев, В. Н. Военная стратегия США после холодной войны / В. Н. Конышев. – СПб. : Наука, 2009. – С. 85–86.

2. Головко, В. А. Основы компьютерных технологий : учеб.-метод. пособие / В. А. Головко, А. А. Дудкин, Л. П. Матюшков. – Брест : БрГТУ, 2015. – 180 с.

3. Молдовян, А. А. Новые алгоритмы и протоколы для аутентификации информации в АСУ / А. А. Молдовян, Н. А. Молдовян // Автоматика и телемеханика. – 2008. – Вып. 7. – С. 157–169.

УДК 519.24

Е. И. Мирская
Беларусь, Брест, БрГУ имени А. С. Пушкина

ИССЛЕДОВАНИЕ ОЦЕНКИ СПЕКТРАЛЬНОЙ ПЛОТНОСТИ МНОГОМЕРНОГО ВРЕМЕННОГО РЯДА

Исследование статистических оценок спектральных плотностей является одной из классических задач анализа временных рядов. В данной работе в качестве оценки неизвестной спектральной плотности многомерного временного ряда исследована статистика, построенная по методу Уэлча.

Предположим, что число наблюдений T за процессом $X(t)$, $t \in Z$ представимо в виде: $T = L\,[r(N-1)+1]$, где $r \in \{1,2,...\}$, $N \in \{1,2,...\}$, L – число непересе-

кающихся интервалов разбиения, содержащих по $r\,(N-1)$ наблюдений. В качестве оценки неизвестной спектральной плотности исследована статистика вида

$$\tilde{f}_{N,r}(\lambda)=\frac{1}{L}\sum_{l=0}^{L-1} I_{N,r}(\lambda,l), \qquad (1)$$

$\lambda\in\Pi$, построенная путем осреднения расширенных периодограмм по L непересекающимся интервалам наблюдений.

В работе также исследована статистика, построенная по пересекающимся интервалам наблюдений. Предположим, что число наблюдений $T=S\left[\left(r(N-1)+1\right)M\right]+M$, $r\in\{1,2,...\}$, где S – число пересекающихся интервалов разбиения длины N, $0\le M<N$. В качестве оценки неизвестной взаимной спектральной плотности процесса исследована статистика вида

$$f_{N,r}(\lambda)=\frac{1}{S}\sum_{s=1}^{S} I_{N,r}(\lambda,s), \qquad (2)$$

где

$$I_{N,r}(\lambda,s)=\left|d_{N,r}(\lambda,s)\right|^2,$$

$$d_{N,r}(\lambda,s)=\frac{1}{\sqrt{H^s_{N,r}}}\sum_{t=(s-1)\left[r(N-1)+1\right]-M}^{s\left(\left[r(N-1)+1\right]-M\right)+M-1} Q_{N,r}(t-(s-1)[r(N-1)+1-M])X(t)e^{-i\lambda t}.$$

$s=\overline{1,S},\lambda\in\prod,t\in Z$, функция $Q_{N,r}(t)$ определяется как решение уравнения

$$\sum_{t=0}^{r(N-1)} Q_{N,r}(t)e^{it\alpha}=\left(\sum_{t=0}^{N-1} e^{it\alpha}\right)^r,$$

$$H^s_{N,r}=2\pi\sum_{t=(s-1)\left[r(N-1)+1\right]-M}^{s\left(\left[r(N-1)+1\right]-M\right)+M-1} Q^2_{N,r}(t-(s-1)[r(N-1)+1-M]).$$

УДК 336:51:004

Д. А. Петрукович
Беларусь, Брест, БрГУ имени А. С. Пушкина

КОМПЬЮТЕРНАЯ ПОДДЕРЖКА МАТЕМАТИЧЕСКОЙ ПОДГОТОВКИ ЭКОНОМИСТОВ КАК ЭЛЕМЕНТ ПРОФЕССИОНАЛЬНОЙ НАПРАВЛЕННОСТИ ОБУЧЕНИЯ

Переход на четырехлетнее обучения на первой ступени получения высшего образования потребовал ускорения процесса профессиональной направленности обучения математическим дисциплинам, эффективной актуализации математических знаний при изучении общепрофессиональных дисциплин и формированию устойчивых академических, социально-личностных и профессиональных компетенций. К содержанию профессиональных компетенций относится выработка у обучающихся способности к овладению и профессиональному применению современных информационных технологий.