7. Дернова Е. С., Молдовян Н. А. Синтез алгоритмов цифровой подписи на основе нескольких вычислительно трудных задач // Вопр. защиты информации. 2008. № 1. С. 22–26.

8. Дернова Е. С., Молдовян Н. А. Протоколы коллективной цифровой подписи, основанные на сложности решения двух трудных задач // Безопасность информационных технологий. 2008. № 2. С. 79–85.

9. Молдовян Н. А. Практикум по криптосистемам с открытым ключом. СПб.: БХВ-Петербург, 2007.

10. Tahat N. M. F., Ismail E. S., Ahmad R. R. A New Blind Signature Scheme Based on Factoring and Discrete Logarithms // Intern. J. of Cryptology Research. 2009. Vol. 1. P. 1–9.

A. N. Berezin, N. A. Moldovyan

CRYPTOSCHEME DESIGN BASED ON THE PROBLEM OF DISCRETE LOGARITHM MODULO A NUMBER DIFFICULT FOR FACTORING

In order to improve security, a justification have been given for designing the public-key algorithms and protocols based on difficulty of finding discrete logarithm modulo in case of using a composite number that is difficult for factoring. It is proposed to use the product of two strong primes as the modulo, with their sizes relation 2:1. This approach provides an alternative solution for construction of the cryptoschemes, based on difficulty of simultaneous solving both the discrete logarithm modulo prime problem and the factoring problem. The approach provides reducing the signature size in digital signature protocols and increasing the rate of the cryptoschemes.

Cryptographic protocol, digital signature, blind collective signature, factoring problem, discrete logarithm problem, public key

УДК 658.512.22

Р. И. Сольницев, До Суан Чо, Б. И. Шапошинков

К ОЦЕНКЕ ТОЧНОСТИ ОБРАБОТКИ МЕТЕОРОЛОГИЧЕСКИХ ДАННЫХ В ЗАМКНУТОЙ СИСТЕМЕ УПРАВЛЕНИЯ «ПРИРОДА – ТЕХНОГЕНИКА»

Рассматриваются вопросы построения подсистемы САПР метеорологической поддержки (МП) замкнутой системы управления «природа – техногеника» (ЗСУ ПТ). Представлены алгоритмы оценки точности обработки метеорологических данных в ЗСУ ПТ. Приведены численные результаты такой оценки.

Экология, загрязняющие вещества, метеорологическое обеспечение, алгоритм, оценка точности, нестационарный случайный процесс, подсистема САПР

В предыдущих работах [1], [2] проведен анализ основных подходов к построению ЗСУ ПТ с целью минимизации загрязняющих веществ (ЗВ) в атмосфере, рассмотрено решение задач синтеза управлений, разработки САПР ЗСУ ПТ. В частности, в [2] рассмотрены вопросы метеорологической поддержки ЗСУ ПТ. Для управления в ЗСУ ПТ необходимо обеспечить поступление метеоданных в ЗСУ ПТ в режиме реального времени.

Известно, что метеорологические данные по ветру, температуре, давлению, влажности (v, T, p, W), полученные из Центра метеорологической информации района, промзоны, в общем случае являются нестационарными случайными процессами (НСП). Однако при оценках статистических характеристик реализаций в процессе обработки метеоданных непосредственное использование этих данных затруднено вследствие малого количества реализаций, полученных на практике.

С целью приближения алгоритмов обработки метеоданных и формирования управляющих воздействий в ЗСУ ПТ к хорошо разработанным и удобным характеристикам стационарных эргодических процессов обработка и ввод в ЗСУ ПТ метеоданных проводятся по эквивалентным статистическим характеристикам стационарных процессов с оценками этих характеристик на стационарность и эргодичность.

В работе [2] приведены алгоритмы и результаты обработки метеоданных как НСП по одной реализации и их приведения к эквивалентному стационарному процессу. В данной статье представлены оценки точности такого приведения.

Для каждой реализации $x_i(t)$ НСП $X(t)$ определяется средняя корреляционная функция по формуле

$$R^i_{X_{\text{ср}}}(\lambda) = \frac{1}{T_0}\int_0^{T_0} R^i_X(t+\lambda)dt,$$

где T_0 – время усреднения корреляционной функции $R^i_X(t,\lambda)$.

Измерение корреляционной функции $R^i_X(t,\lambda)$ центрированного НСП $X(t)$ по каждой реализации проводится методом текущего (скользящего) усреднения в соответствии с выражением

$$R^i_X(t,\lambda) = \frac{1}{T_{\text{и}}}\int_{t-\frac{T_{\text{и}}}{2}}^{t+\frac{T_{\text{и}}}{2}} x_i(t)\,x_i(t+\lambda)dt, \qquad (1)$$

где $T_{\text{и}}$ – интервал текущего усреднения.

Интервал $T_{\text{и}}$ определяется исходя из требуемой точности измерения оценки корреляционной функции $R^i_X(t,\lambda)$. С целью такой оценки введем показатель

$$\gamma^2_R = \frac{d^2_R}{D^2_{X_{\text{ср}}}}, \qquad (2)$$

где

$$d_R = \sqrt{M\left\{\left[R^i_X(t,\lambda) - R_{X_0}(t,\lambda)\right]^2\right\}} \qquad (3)$$

– среднеквадратическая погрешность оценки $R^i_X(t,\lambda)$; $D_{X_{\text{ср}}} = \frac{1}{T_0}\int_0^{T_0} D_{X_0}(t)\,dt$ – среднее значение текущей дисперсии $D_{X_0}(t)$ ($R_{X_0}(t,\lambda)$ – корреляционная функция i-й реализации, построенная по экспериментальным данным сглаживания; M – символ математического ожидания).

Покажем применение формулы (2) на примере вычисления оценки точности статистических характеристик скорости ветра (v).

Поскольку число реализаций i в ансамблях по (v) как правило мало, то обработка ведется по одной реализации достаточной длины с соответствующими оценками на эргодичность и интервалов сглаживания $T_{\text{и}}$ по соотношениям (1), (2).

На рис. 1 представлена исходная реализации скорости ветра $v(t)$ за год (2011 г.). В табл. 1 приведен результат построения соответствующей корреляционной функции $v(t)$ на основе известного алгоритма обработки НСП [3] с нормальной функцией распределения плотности вероятности.

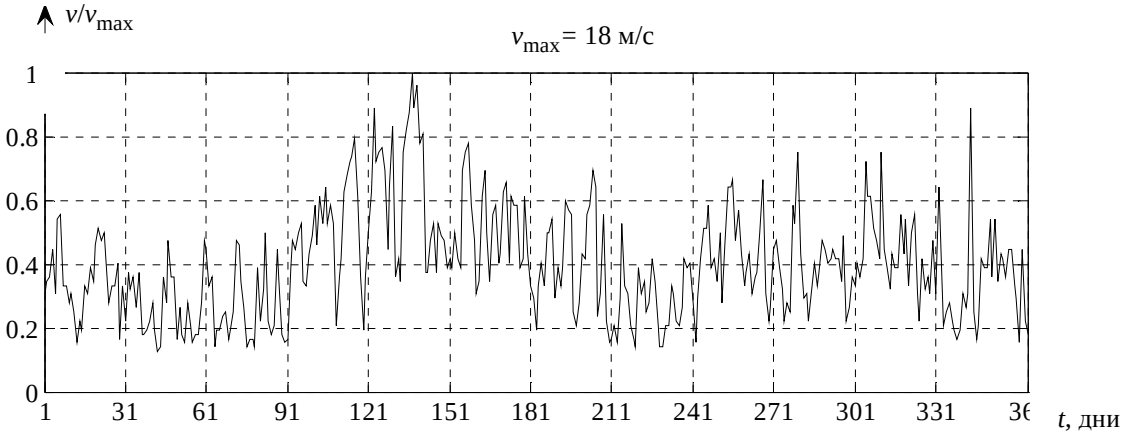

Рис. 1

Таблица 1

λ, день	*t*, день								
	1	2	3	4	5	6	7	….	365
1	0,013	0,040	–0,019	–0,092	0,123	0,034	0,055	…	0,760
2	0,043	0,010	0,170	0,064	–0,036	–0,095	–0,039	…	0,680
3	– 0,026	0,046	0,186	0,181	0,071	–0,051	–0,015	…	0,489
…	…	…	…	…	…	…	…	…	…
100	0,080	0,170	0,350	0,123	…	…	…	…	0,214

Для расчетов по формуле (3) функция $R^i_{X_0}(t,\lambda)$ аппроксимируется в среде Matlab 2011b средствами Matlab Curve Fitting Tool. Аналитическое представление этой корреляционной функции имеет вид

$$R_{X_0}(t,\lambda) = D_{X_{\text{ср}}}\left(1+b\cos\left(w_0\, t\right)\right)^2 e^{-\alpha|\lambda|}\cos\left(w\,\lambda\right). \tag{4}$$

В табл. 2 показаны численные оценки параметров аппроксимации (4) автокорреляционной функции $R^i_{X_0}(t,\lambda)$.

Таблица 2

Параметр	Среднее	Минимальное значение	Максимальное значение
$D_{X\text{ср}}$	0,5584	0,5438	0,5730
b	0,0071	0,0011	0,0132
α	0,0100	0,0081	0,0119
w_0	0,0311	0,0308	0,0312
w	0,2196	0,2155	0,2236

Расчет по формуле (3) приводит к значению d_R = 0,0741.

В соответствии с выражением (4) оценка γ_R имеет вид [4]:

$$\gamma_R^2 \le \frac{1}{2T_{\text{и}}\left(\alpha^2+w^2\right)}\left\{2\alpha T_{\text{и}} + \frac{1}{\alpha^2+w^2}\left[\left(w^2-\alpha^2\right)\left(1-e^{-2\alpha T_{\text{и}}}\cos 2wT_{\text{И}}\right) - 2\alpha w e^{-2\alpha T_{\text{и}}}\sin 2wT_{\text{и}}\right]\right\} +$$

$$+ \frac{b^2 {T_{\text{и}}}^4 {w_0}^4}{24^2}.$$

Оценить значение $T_{\text{и}}$ можно по приближенной формуле

$$\gamma_R^2 \le \frac{1+2\alpha T_{\text{и}}}{2{T_{\text{и}}}^2 w^2} + \frac{b^2 {T_{\text{и}}}^4 {w_0}^4}{24^2}, \tag{5}$$

$$e^{-\alpha T_{\text{И}}} << 1 \text{ при } w >> \alpha. \tag{6}$$

Значения γ_R, $T_{\text{и}}$, вычисленные по формулам (2) и (5), (6): $\gamma_R = 13,28\,\%$, $T_{\text{и}} = 100$ дней.

Для оценки отклонения составляющих $R_X^i\left(t, \lambda_j\right)$ от среднего значения $R_{X_{\text{ср}}}^i\left(\lambda_j\right)$ применяется показатель нестационарности:

$$\gamma_{\text{н}}^2 = \frac{D_R^2}{D_{X_{\text{ср}}}^2}, \tag{7}$$

где $D_R = \sum_{j=0}^{n} \frac{D_{jR}}{n+1}$ – дисперсия отклонения корреляционной функции $R_X^i\left(t, \lambda_j\right)$ от средней корреляционной функции $R_{X_{\text{ср}}}^i\left(\lambda\right)$; $D_{X_{\text{ср}}}$ – среднее значение оценки $D_X(t)$;

дисперсия отклонения j-й составляющей $R_X^i\left(t, \lambda_j\right)$ от $R_{X_{\text{ср}}}^i\left(\lambda_j\right)$:

$$D_{jR} = \frac{1}{T_0} \int_0^{T_0} \left[R_X^i\left(t, \lambda_j\right) - R_{X_{\text{ср}}}^i\left(\lambda_j\right) \right]^2 dt. \tag{8}$$

Показатель $\gamma_{\text{н}}$ служит для численной оценки близости анализируемого НСП к эквивалентному стационарному случайному процессу.

Обработка проводилась в среде MATLAB R2011b MathWorks при помощи программного обеспечения подсистемы САПР МП ЗСУ ПТ.

Результат вычисления показателя нестационарности на основе алгоритмов (7), (8): $D_{X_{\text{ср}}} = 0,7751$, $\gamma_{\text{н}} = 16,27\,\%$.

Таким образом, предложенные в статье алгоритмы и численные результаты показывают достаточную точность обработки и передачи метеорологических данных в ЗСУ ПТ.

СПИСОК ЛИТЕРАТУРЫ

1. Сольницев Р. И., Коршунов Г. И. Системы управления «Природа – Техногеника». СПб.: Политехника, 2013.
2. Сольницев Р. И., До Суан Чо. Алгоритмизация обработки и передачи метеорологических данных в Замкнутой системе управления «Природа-техногеника»// Информационно-управляющие системы. 2013. № 3. С. 30–35.
3. Лившиц Н. А., Пугачев В. С. Вероятностный анализ систем автоматического управления. М.: Сов. радио, 1963.
4. Об измерении средней корреляционной функции нестационарного случайного процесса по одной реализации / Р. И. Сольницев, В. Ф. Рысенко, Л. Л. Шалыт, С. А. Харитонеко // Изв. вузов. «Приборостроение». 1972. Т. 15, № 4. С. 71–75.

R. I. Solnitsev, Do Xuan Cho, B. I. Shaposhinkov

TO THE ACCURACY ESTIMATION OF METEOROLOGICAL DATA PROCESSING IN THE CLOSED CONTROL SYSTEM “NATURE - TECHNOGENIC” (CCS NT)

This article discusses the questions of construction of subsystems CAD meteorological support (MS) the closed control system "Nature-Technogenic" (CCS NT). Algorithms of assess the accuracy of meteorological data processing in CCS NT. The numerical results of of such an assessment.

Ecology, pollutants, meteorological support, algorithm, evaluation of the accuracy, no stationary random process, subsystem CAD