МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 3, № 2

Volume 3, No. 2

Одеса – 2013
Odesa – 2013

Журнал внесений до переліку наукових фахових видань України
(технічні науки)
згідно наказу Міністерства освіти і науки України № 463 від 25.04.2013 р.

Виходить 4 рази на рік

Заснований Одеським національним політехнічним університетом у 2011 році

Свідоцтво про державну реєстрацію КВ № 17610 - 6460Р від 04.04.2011р.

Головний редактор: *Г.О. Оборський*

Заступник головного редактора: *А.А. Кобозєва*

Відповідальний редактор: *І.І. Бобок*

Published 4 times a year

Founded by Odessa National Polytechnic University in 2011

Certificate of State Registration КВ № 17610 - 6460P of 04.04.2011

Editor-in-chief: *G.A. Oborsky*

Associate editor: *A.A. Kobozeva*

Executive editor: *I.I. Bobok*

Друкується за рішенням редакційної колегії та Вченої ради Одеського національного політехнічного університету

Оригінал-макет виготовлено редакцією журналу

Адреса редакції: просп. Шевченка, 1, Одеса, 65044, Україна

Телефон: +38 048 734 8506

Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com

Editorial address: 1 Shevchenko Ave., Odessa, 65044, Ukraine

Tel.: +38 048 734 8506

Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com

ЗМІСТ / CONTENTS

УДК 621.396.664:681.5.015.52

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 2, pp. 103-112

ОПТИМИЗАЦИЯ ВЫЧИСЛИТЕЛЬНЫХ АЛГОРИТМОВ АППРОКСИМАЦИОННОГО МЕТОДА ИДЕНТИФИКАЦИИ НЕЛИНЕЙНЫХ СИСТЕМ В ВИДЕ МОДЕЛЕЙ ВОЛЬТЕРРА

С.В. Павленко, С.А. Положаенко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, e-mail: psv85@yandex.ru

Рассматривается аппроксимационный метод детерминированной идентификации нелинейных динамических систем в виде моделей Вольтерра. Получена оценка сверху погрешности идентификации, значение которой зависит от выбора амплитуд тестовых воздействий. Приведены значения оптимальных амплитуд тестовых сигналов и соответствующих масштабирующих коэффициентов в вычислительных алгоритмах метода идентификации. Для тестового объекта получены оценки сечений ядер Вольтерра второго и третьего порядков при использовании в качестве тестовых нерегулярных последовательностей импульсов. Для сглаживания полученных результатов идентификации применяется вейвлет-фильтрация.

Ключевые слова: идентификация, аппроксимационный метод, вычислительные алгоритмы, оптимизация, нелинейные системы, модели Вольтерра, импульсные тестовые сигналы, вейвлет-преобразования

Введение

Интегростепенные ряды Вольтерра (РВ) [1–3] в последнее время становятся все более распространенным аппаратом исследования нелинейных динамических систем (НДС) [4]. Это объясняется целым рядом положительных свойств РВ – универсальностью, возможностью аналитического описания динамических свойств систем, использованием многих привычных для инженера понятий теории линейных систем (многомерных импульсных переходных и передаточных функций), уникальностью – в некоторых случаях они являются иногда единственным инструментом исследования.

Задача построения модели НДС в виде РВ (задача идентификации) заключается в выборе вида тестовых воздействий и разработке алгоритма, который позволял бы по измеренным реакциям системы определять многомерные импульсные переходные функции – ядра Вольтерра (ЯВ) или передаточные функции – Фурье–изображения ЯВ соответственно для моделирования системы во временной или частотной областях [5]. Если в исследуемой системе необходимо оценивать характер искажений формы сигналов, то используется временная область и определяются многомерные ЯВ. Если же требуется проводить анализ частотных искажений, то, очевидно, при моделировании системы эффективнее использовать частотную область и определять многомерные передаточные функции.

В [5] предложен аппроксимационный метод идентификации НДС, который основывается на выделении в отклике НДС n-ой парциальной составляющей (ПС) РВ с помощью построения линейных комбинаций откликов на тестовые сигналы с разными амплитудами. В [6] дано теоретическое обоснование аппроксимационного метода

детерминированной идентификации НДС на основе моделей Вольтерра во временной области с использованием в качестве тестовых сигналов нерегулярных последовательностей импульсов. При применении метода получаем оценки диагонального и поддиагональных сечений многомерных ЯВ. Погрешность оценки сечений ЯВ зависит от выбора амплитуд импульсов тестовых последовательностей и значений масштабирующих коэффициентов откликов при обработке экспериментальных данных [5–8].

Целью работы является оптимизация вычислительных алгоритмов аппроксимационного метода идентификации нелинейных динамических систем на основе моделей Вольтерра, позволяющая минимизировать погрешность оценки сечений ядер Вольтерра при использовании тестовых нерегулярных импульсных последовательностей.

Модели Вольтерра и аппроксимационный метод идентификации нелинейных систем

Соотношение «вход–выход» для непрерывной НДС с неизвестной структурой (типа «черный ящик») с одним входом и одним выходом может быть представлено рядом Вольтерра в виде

$$y(t) = w_0(t) + \int_0^t w_1(\tau)x(t-\tau)d\tau + \int_0^t\int_0^t w_2(\tau_1,\tau_2)x(t-\tau_1)x(t-\tau_2)d\tau_1\,d\tau_2 + \\ + \int_0^t\int_0^t\int_0^t w_3(\tau_1,\tau_2,\tau_3)x(t-\tau_1)x(t-\tau_2)x(t-\tau_3)d\tau_1\,d\tau_2\,d\tau_3 + \ldots = w_0(t) + \sum_{n=1}^{\infty} y_n[x(t)], \quad (1)$$

где

$y_n[x(t)] = \int_0^t \ldots \int_0^t w_n(\tau_1,\ldots,\tau_n)\prod_{i=1}^{n} x(t-\tau_i)d\tau_i$ — n–мерный интеграл свертки, n-ая парциальная составляющая (ПС) отклика системы $y(t)$;

$x(t)$ — входной сигнал системы;

$w_n(\tau_1,,\ldots,\tau_n)$ — ядро Вольтерра или весовая функция n-го порядка ($n = 1,2,3,\ldots$) — симметричная относительно действительных переменных $\tau_1,,\ldots,\tau_n$ функция;

$w_0(t)$ — свободный член ряда (при нулевых начальных условиях $w_0(t) \equiv 0$);

t — текущее время.

Аппроксимационный метод детерминированной идентификации НДС основан на выделении в отклике НДС n-ой ПС с помощью построения линейных комбинаций откликов на тестовые сигналы с разными амплитудами. В [8] доказано

Утверждение. Пусть на вход системы поочередно подаются тестовые сигналы $a_1x(t), a_2x(t), \ldots, a_Nx(t)$ (N — порядок аппроксимационной модели; $a_1, a_2, \ldots, a_N$ — различные вещественные числа, удовлетворяющие условию $0 < |a_j| \le 1$ для $\forall j = \overline{1,N}$; $x(t)$ — произвольная функция), тогда линейная комбинация откликов НДС на эти воздействия равна m-ой ПС отклика на входной сигнал $x(t)$ с погрешностью Δ, обусловленной членами РВ порядка выше N-го:

$$\sum_{j=1}^{N} c_j y[a_j x(t)] = y_m[x(t)] + \Delta, \quad (2)$$

где c_j — действительные коэффициенты, такие что удовлетворяют системе линейных алгебраических уравнений (СЛАУ), запись которых в векторно-матричной форме имеет вид

$$\mathbf{A} \cdot \mathbf{c} = \mathbf{b}, \tag{3}$$

здесь

$$\mathbf{A} = \begin{bmatrix} a_1 & a_2 & \dots & a_N \\ a_1^2 & a_2^2 & \dots & a_N^2 \\ \dots & \dots & \dots & \dots \\ a_1^m & a_2^m & \dots & a_N^m \\ \dots & \dots & \dots & \dots \\ a_1^N & a_2^N & \dots & a_N^N \end{bmatrix}, \quad \mathbf{c} = \begin{bmatrix} c_1 \\ c_2 \\ \dots \\ c_m \\ \dots \\ c_N \end{bmatrix}, \quad \mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \\ \dots \\ b_m \\ \dots \\ b_N \end{bmatrix},$$

причем $b_m = 1$ при $n = m$ и $b_n = 0$ при $n \neq m$, $n = \overline{1, N}$, $\forall m \in \{1, 2, \dots, N\}$;

$$\Delta = \sum_{j=1}^{N} c_j \sum_{n=N+1}^{\infty} y_n\left[a_j x(t)\right]. \tag{4}$$

Выделенная ПС $y_m\left[x(t)\right]$ используется для определения ЯВ *m*-го порядка ($1 \le m \le N$).

Поскольку СЛАУ (3) всегда имеет решение, причем единственное, так как ее определитель только множителем $a_1 a_2 \dots a_N$ отличается от определителя Вандермонда, то при любых вещественных числах a_j, отличных от нуля и попарно различных, можно найти такие числа c_j, при которых линейная комбинация (2) из откликов НДС равна *m*-му члену РВ с точностью до отброшенных членов порядка $N+1$ и выше.

Оптимизация выбора амплитуд тестовых сигналов

Выбор амплитуд a_j должен обеспечивать сходимость ряда (1) и минимум погрешности при выделении ПС $y_m\left[x(t)\right]$ в соответствии с (2), определяемой остатком ряда – членами ряда степени $N+1$ и выше. Если $x(t)$ — тестовое воздействие максимально допустимой амплитуды, при котором ряд (1) сходится, то амплитуды a_j должны быть по модулю не больше единицы

$$\left|a_j\right| \le 1 \quad \text{для} \quad \forall j = \overline{1, N}. \tag{5}$$

Чем больше *N*, тем меньше влияние отброшенных членов РВ и тем больше проводится тестовых испытаний.

В [8] показано, что предложенные в [5] для использования в аппроксимационном методе идентификации амплитуды тестовых сигналов не являются оптимальными и не обеспечивают минимум погрешности оценки многомерных ЯВ идентифицируемой системы. Для минимизации влияния остатка РВ на погрешность выделения ПС отклика НДС (4) необходимо обеспечить минимум суммы модулей коэффициентов c_j ($j = \overline{1, N}$), которые определяются из системы уравнений (3)

$$\varepsilon = \sum_{j=1}^{N} \left| c_j \right| = \sum_{j=1}^{N} \left| a_{jk}^{-1} \right| = \min \ , \qquad (6)$$

где a_{jk}^{-1} — элемент матрицы, обратной **A**.

В соответствии с (6) задача обеспечения минимума методической ошибки при применении аппроксимационного метода идентификации сводится к нахождению локальных минимумов функции многих переменных, т.е. суммы модулей коэффициентов c_j. С помощью процедуры полного перебора различных значений амплитуд, решением каждый раз для них СЛАУ (3), вычисляются соответствующие им коэффициенты. Находя минимальное значение выражения (6), определяются оптимальные значения амплитуд $a_1, a_2, \ldots, a_N$ для заданных параметров m и N метода идентификации. Интервал поиска задаётся неравенствами (5). Полученные оптимальные значения амплитуд тестовых воздействий для различных порядков аппроксимационной модели $N = 1 \ldots 6$ и определяемых ЯВ $1 \le m \le N$ приведены в табл. 1 (интервал поиска [-1,1]) и табл. 2 (интервал поиска [0,1]).

Таблица 1.

Оптимальные амплитуды тестовых сигналов на интервале [-1;1]

N	m	$a_j,\ j = \overline{1,N}$	$c_j,\ j = \overline{1,N}$	$\min \sum_{j=1}^{N} \left| c_j \right|$
1	2	3	4	5
1	1	1	-1	1
2	1	-1	-0.5	1
		1	0.5	
	2	-1	0.5	1
		1	0.5	
3	1	-1	0.33	3
		-0.5	-2	
		0.5	0.67	
	2	-1	0.5	1
		0	0	
		1	0.5	
	3	-1	-0.33	4
		0.5	-2.67	
		1	1	

Продолжение таблицы 1.

1	2	3	4	5
4	1	-1	0.17	3
		-0.5	-1.33	
		0.5	1.33	
		1	-0.17	
	2	-1	-0.35	4.83
		-0.64	2.06	
		0.64	2.06	
		1	-0.35	
	3	-1	-0.67	4
		-0.5	-1.33	
		0.5	-1.33	
		1	0.67	
	4	-1	0.85	5.83
		-0.64	-2.06	
		0.64	-2.06	
		1	0.85	
5	1	-1	-0.18	5.01
		-0.8	0.51	
		-0.3	-2.77	
		0.3	1.5	
		0.8	-0.06	
	2	-1	-0.28	4.9
		-0.6	2.17	
		-0.5	0	
		0.6	2.17	
		1	-0.28	
	3	-1	1.87	20.03
		-0.8	-5.38	
		-0.3	10.92	
		0.8	1.5	
		1	-0.36	
	4	-1	0.78	5.9
		-0.6	-2.17	
		0.6	-2.17	
		0.9	0	
		1	0.78	
	5	-1	-1.98	16.03
		-0.8	4.34	
		-0.3	-6.66	
		0.8	-1.97	
		1	1.07	

Продолжение таблицы 1.

1	2	3	4	5
6	1	-1	-0.09	5.01
		-0.8	0.28	
		-0.3	-2.13	
		0.3	2.13	
		0.8	-0.28	
		1	0.09	
	2	-1	0.41	11.68
		-0.9	-0.8	
		-0.4	4.64	
		0.4	4.64	
		0.9	-0.8	
		1	0.41	
	3	-1	1.11	20.03
		-0.8	-3.44	
		-0.3	5.46	
		0.3	-5.46	
		0.8	3.44	
		1	-1.11	
	4	-1	-3.04	38.39
		-0.9	5.8	
		-0.4	-10.36	
		0.4	-10.36	
		0.9	5.8	
		1	-3.04	
	5	-1	-1.53	16.03
		-0.8	3.16	
		-0.3	-3.33	
		0.3	3.33	
		0.8	-3.16	
		1	1.53	
	6	-1	1.65	27.85
		-0.8	7.75	
		-0.4	1.65	
		0.4	7.75	
		0.8	-4.52	
		1	-4.52	

Таблица 2.

Оптимальные амплитуды тестовых воздействий на интервале [0;1]

N	m	$a_j,\ j=\overline{1,N}$	$c_j,\ j=\overline{1,N}$	$\min\sum_{j=1}^{N}\lvert c_j\rvert$
1	1	1	1	1
2	1	0	0	1
		1	1	
	2	0.41	-4.13	5.82
		1	1.69	
3	1	0.75	-1.93	11.21
		1	0.75	
		0.2	8.52	
	2	0.75	11.63	36.27
		1	-4.75	
		0.2	-19.88	
	3	0.2	11.36	26.06
		0.75	-9.69	
		1	5	

Оценка сечений многомерных ядер Вольтерра

При использовании сигналов $x(t)$, представляющих собой нерегулярные импульсные последовательности, оценка поддиагонального сечения ЯВ *n*-го порядка НДС [6, 8]

$$\hat{w}_n(t-\tau_1,...,t-\tau_n)=\frac{(-1)^n}{n!(\Delta\tau)^n}\sum_{\delta_1,...,\delta_n=0}^{1}(-1)^{\sum_{i=1}^{n}\delta_i}\hat{y}_n(t,\delta_1,...,\delta_n), \tag{7}$$

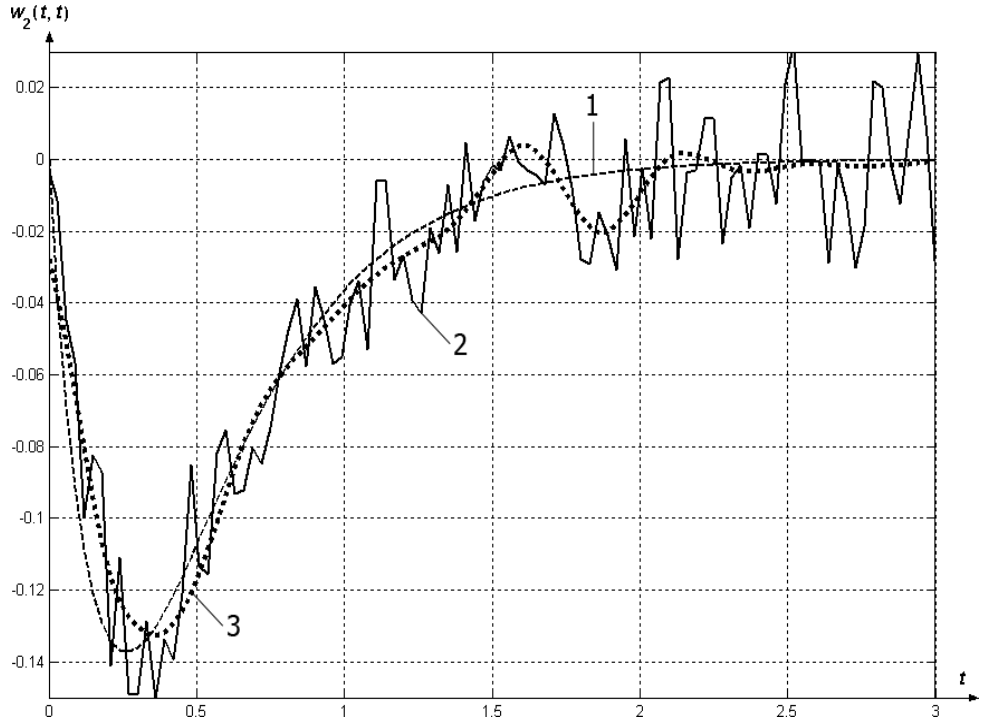
где $\hat{y}_n(t,\delta_1,...,\delta_n)$ — оценка *n*-ой ПС отклика НДС в момент времени *t*, полученная в результате обработки данных экспериментов на основе (2), при действии на входе нерегулярной последовательности импульсов: если $\delta_i=1$, то на входе НДС в момент времени τ_i есть импульс, при $\delta_i=0$ – импульс отсутствует.

Оценка диагонального сечения ЯВ *n*–го порядка

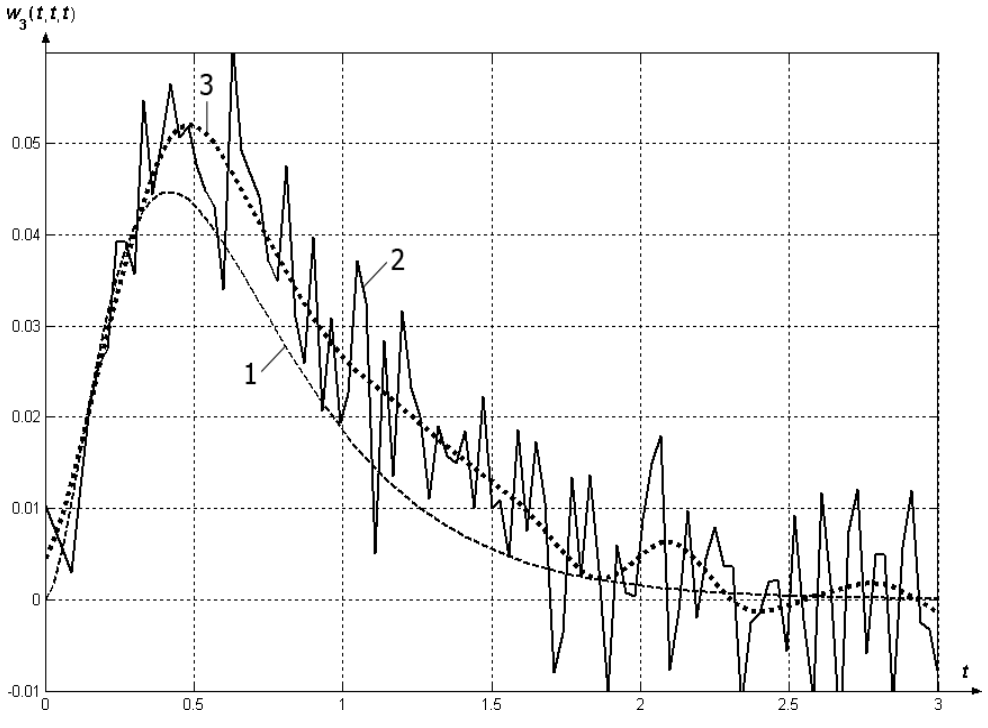
$$\hat{w}_n(t,t,...,t)=\frac{\hat{y}_n(t)}{(\Delta\tau)^n}, \tag{8}$$

где $\hat{y}_n(t)$ — оценка *n*-ой ПС отклика НДС на одиночный импульс в момент времени *t*, полученная в результате обработки данных экспериментов (2).

На рис. 1 для тестового объекта представлены результаты идентификации диагональных сечений ЯВ второго (а) и третьего (б) порядков НДС с использованием аппроксимационного метода при $N=4$ и погрешности измерений 1%, полученные с помощью компьютерного моделирования. Для сглаживания полученных результатов идентификации применяется вейвлет-фильтрация [9, 10].



а



б

Рис. 1. Результат идентификации диагональных сечений ЯВ второго (а) и третьего (б) порядков НДС с помощью аппроксимационного метода ($N = 4$) при погрешности измерений 1%: эталонные ЯВ (1); идентифицированные ЯВ (2); идентифицированные ЯВ при применении вейвлет–фильтрации на основе вейвлета *coif4* с уровнем разложения $L = 4$ (3)

Выводы

Усовершенствован аппроксимационной метод идентификации нелинейных динамических систем на основе моделей Вольтерра. Модификация метода заключается в выборе амплитуд тестовых сигналов и соответствующих масштабирующих коэффициентов в процедуре обработки сигналов-откликов, основанном на минимизации методической погрешности выделения парциальных составляющих из отклика объекта идентификации, что позволяет получать оценки ядер Вольтерра с более высокой точностью как во временной, так и в частотной области. Для повышения вычислительной устойчивости алгоритмов идентификации применяются процедуры шумоподавления к получаемым оценкам многомерных ядер Вольтерра, основанные на вейвлет-преобразовании, что позволяет получить сглаженные решения и уменьшить погрешность идентификации в 1.5–3 раза.

Список литературы

1. Третьяк, А.И. Дифференциально-геометрические методы в теории дискретных систем управления [Текст] : монография / А.И. Третьяк, А.В. Усов, А.П. Коновалов. — Одесса : Астропринт, 2008. — 358 с.
2. Методы классической и современной теории автоматического управления [Текст] : в 5 т.: учеб. для вузов по машиностроит. и приборостроит. специальностям / под ред. К.А. Пупкова, Н.Д. Егупова. — Изд. 2., перераб. и доп. — М. : Изд-во МГТУ им. Н.Э. Баумана, 2004 — . —
   Т. 2 : Статистическая динамика и идентификация систем автоматического управления / [К.А. Пупков, Н.Д. Егупов, А.И. Баркин и др.]. — 2004. — 638 с.
3. Doyle, F.J. Identification and Control Using Volterra Models / F.J. Doyle III, R.K. Pearson, and B.A. Ogunnaike. — London ; New York : Springer, 2002. — 314 p.
4. Giannakis, G.B. A bibliography on nonlinear system identification / G.B. Giannakis, E. Serpedin // Signal Processing. —Elsevier Science B.V., 2001. — Vol. 81, Iss. 3. — PP. 533–580.
5. Данилов, Л.В. Теория нелинейных электрических цепей [Текст] / Л.В. Данилов, П.Н. Матханов, Е.С. Филиппов. — Л. : Энергоатомиздат. Ленингр. отд-ние, 1990. — 252 с.
6. Павленко, В.Д. Аппроксимационный метод идентификации нелинейных систем на основе моделей Вольтерра с использованием тестовых полиимпульсных сигналов / В.Д. Павленко // Праці Одеського політехнічного університету. — Одесса, 2012. — Вып. 2(39). — С. 237–243.
7. Применение функционального описания Вольтерра для контроля датчиков навигационных систем / В.Н. Попов [и т.д.] // Контроль. Диагностика. — 1999. — № 11. — С. 3–7.
8. Павленко, В.Д. Исследование погрешностей аппроксимационного метода идентификации нелинейных динамических объектов в виде ядер Вольтерра / В.Д. Павленко, С.В. Павленко // Электротехнические и компьютерные системы. — 2010. — № 01(77). — С. 102–108.
9. Павленко, С.В. Применение вейвлет-фильтрации в процедуре идентификации нелинейных систем на основе моделей Вольтерра / С.В. Павленко // Восточно-Европейский журнал передовых технологий. — Харьков: Технологический центр, 2010. — № 6/4(48). — С. 65–70.
10. Смоленцев, Н.К. Основы теории вейвлетов. Вейвлеты в MATLAB : [учеб. пособие для вузов по направлениям подгот. и специальностям «Математика», «Математика. Прикладная математика»] / Н.К. Смоленцев. — 3-е изд., доп. и перераб. — М. : ДМК Пресс, 2008. — 448 с.

ОПТИМІЗАЦІЯ ОБЧИСЛЮВАЛЬНИХ АЛГОРИТМІВ АПРОКСИМАЦІЙНОГО МЕТОДУ ІДЕНТИФІКАЦІЇ НЕЛІНІЙНИХ СИСТЕМ У ВИГЛЯДІ МОДЕЛЕЙ ВОЛЬТЕРРА

С.В. Павленко, С.А. Положаєнко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: psv85@yandex.ru

Розглядається апроксимаційний метод детермінованої ідентифікації нелінійних динамічних систем у вигляді моделей Вольтерра. Отримана оцінка зверху похибки ідентифікації, значення якої залежить від вибору амплітуд тестових впливів. Наведено значення оптимальних амплітуд тестових сигналів і відповідних масштабуючих коефіцієнтів в обчислювальних алгоритмах методу ідентифікації. Для тестового об'єкта отримані оцінки перетинів ядер Вольтерра другого і третього порядків при використанні в якості тестових нерегулярних послідовностей імпульсів. Для згладжування отриманих результатів ідентифікації застосовується вейвлет-фільтрація.

Ключові слова: ідентифікація, апроксимаційний метод, обчислювальні алгоритми, оптимізація, нелінійні системи, моделі Вольтерра, імпульсні тестові сигнали, вейвлет-перетворення

COMPUTING ALGORITHMS OPTIMIZATION OF THE APPROXIMATE METHOD THE IDENTIFICATION OF THE NONLINEAR SYSTEMS IN THE FORM OF VOLTERRA MODELS

Sergey V. Pavlenko, Sergey A. Polozhaenko

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: psv85@yandex.ru

The approximate method of the determined identification of the nonlinear dynamic systems in the form of Volterra models is considered. The assessment from above the identification errors, which depends on a choice of amplitudes test influence is received. Values of optimum amplitudes test signals and the corresponding scaling coefficients were given in computing algorithms of a identification method. There were estimated the sections of the second and the third orders of Volterra kernels which were received in using as test irregular sequences of impulses. The wavelet filtration is applied to smoothing of the received results of identification.

Keywords: identification, approximation method, computational algorithms, optimization, nonlinear systems, Volterra model, impulse test signals, wavelet transform

УДК 621.394.6: 658.62.018

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 2, pp. 113-122

АЛГОРИТМ ТОЧЕЧНОГО ПРОГНОЗИРОВАНИЯ СЛУЧАЙНЫХ ПРОЦЕССОВ В АВИАЦИОННЫХ ИНФОКОММУНИКАЦИОННЫХ СЕТЯХ

Д.В. Чирков, В.Г. Липовский

Национальный авиационный университет,
просп. Космонавта Комарова, 1, Киев, 03680, Украина

В работе рассмотрена общая методика прогнозирующего контроля современных мультисервисных сетей, которая в качестве основного компонента включает алгоритмы структурной идентификации моделей регулярных составляющих (трендов) наблюдаемых процессов. Приведена общая структура методики прогнозирующего контроля авиационных инфокоммуникационных систем. Представлен общий вид алгоритма структурной идентификации.

Ключевые слова: инфокоммуникационные сети, авиационные сети, случайные процессы, точечное прогнозирование, алгоритм прогнозирования, мультисервисные сети

Введение

Решение задач прогнозирующего контроля сводится к принятию решения по предупреждению прогнозируемого отказа.

Поскольку в решаемой задаче информация о том, какие решающие правила являются оптимальными, рассматриваются алгоритмы, позволяющие получать практически приемлемые результаты. Важнейшими условиями обеспечения этого являются:

- построение моделей прогнозирования для конкретных подсетей на основе реальных данных об их функционировании;
- приемлемая глубина контроля, позволяющая в реальных условиях собирать и анализировать измерительную информацию, не сводя деятельность оператора или провайдера исключительно к решению задач контроля;
- привлечение квалифицированных экспертов для формирования прогностических моделей;
- использование алгоритмов прогнозирования, позволяющих решать задачи структурной идентификации с приемлемой точностью, за приемлемое время и отличающихся робастностью – устойчивостью к выбросам реализаций наблюдаемых процессов;
- обеспечение высокой точности прогнозирования, для чего необходимо выполнение принципа максимума воспроизводимости, который ниже и будет рассматриваться как альтернатива принципу максимума правдоподобия.

Таким образом, задачей является синтез единой методики прогнозирующего контроля, включающей организационные, технические, алгоритмические и программные средства, позволяющие решать задачи прогнозирующего контроля с приемлемым качеством для авиационных инфокоммуникационных систем (АИС).

Основная часть

Общая структура методики прогнозирующего контроля приведена на рис. 1.

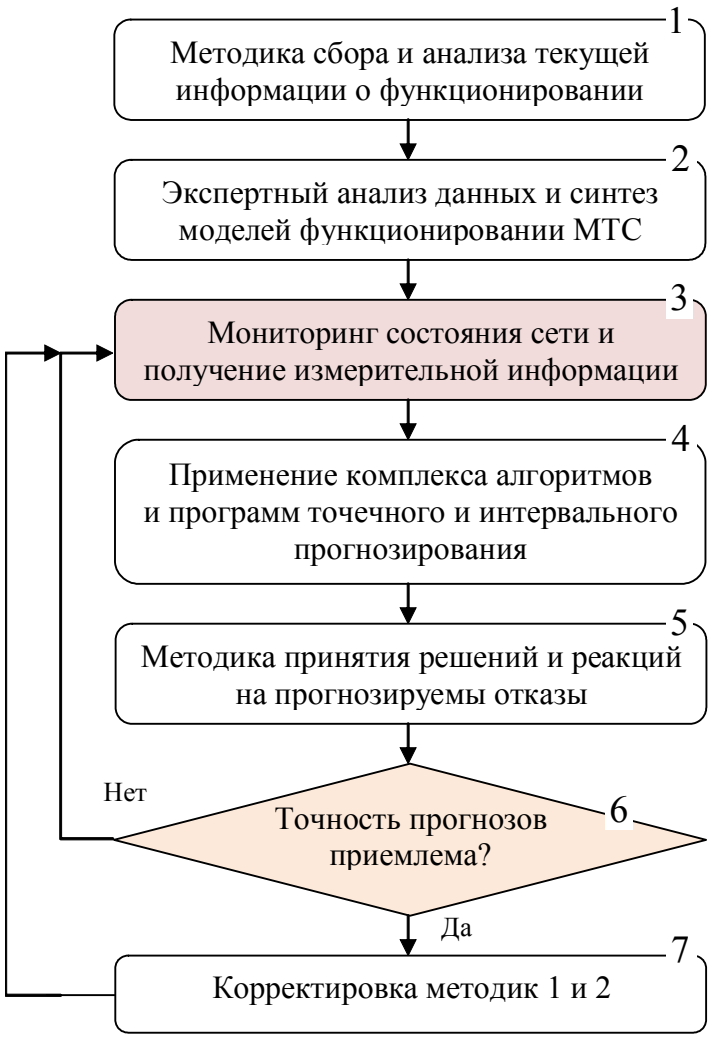


Рис. 1. Общая структура методики прогнозирующего контроля АИС

Разрабатываемая методика, как видим, содержит блоки, декомпозирующие решение общей задачи прогнозирующего контроля на подзадачи, логически вытекающие одна из другой. При этом сама методика представляет собой замкнутую структуру, включающую автоматизируемые и неавтоматизируемые («экспертные») составляющие. При этом должен быть разработан комплекс организационно-технических мероприятий, позволяющий решать задачу прогнозирования отказов с приемлемой точностью.

Рассмотрим по отдельности составляющие методики, приведенной на рис. 1.

Методика сбора и анализа текущей информации о функционировании АИС включает:

1) Методики определения контрольных точек сети, в которой учитывается возможность выполнения прямых или косвенных измерений параметров.

Данная группа методов и средств зависит от конкретной топологии сети. Каждый провайдер (оператор) строит свой центр управления сетью – *network operation centre* (NOC) и выбирает множество контрольных точек сети, исходя из следующих основных положений:

- в обязательном порядке контролируется загрузка портов абонентов выделенных каналов передачи данных;
- в обязательном порядке контролируется загрузка внешних портов, обращенных к портам вышестоящего провайдера;
- данные об отказах типа «непредоставление» услуги фиксируется в диспетчерских журналах.

2) Методики анализа результатов измерений параметров сети, причин возникновения и способов предупреждения отказов.

Экспертный анализ данных и синтез моделей функционировании АИС. Синтезированные в методике модели носят достаточной общий характер и могут применяться для моделирования и прогнозирования параметров реальных сетей с учетом необходимости применения методов структурной идентификации.

Мониторинг состояния сети и получение измерительной информации выполняется на NOC, а также методами периодического контроля и анализа журналов диспетчерских и технических служб.

Применение комплекса алгоритмов и программ точечного и интервального прогнозирования. Разработке такого алгоритмического и программного обеспечения посвящена данная работа.

Методика принятия решений и реакций на прогнозируемые отказы зависит от технической и маркетинговой политики конкретного провайдера. В частности, при планировании внедрения новой услуги, обязательным является оценивания класса QoS, обеспечиваемого данной сетью, прогнозирование возможных отказов с учетом вновь предлагаемого качества и состава услуг, принятие решений о модернизации сети, расширении полос пропускания внешних портов и т.д.

Назначение и смысл фрагментов 6 и 7 общей методики прогностического контроля (рис. 1) очевидны.

Таким образом, рассмотрена общая структура методики прогнозирующего контроля, которая содержит наиболее сложный с научной точки зрения структурный элемент – комплекс алгоритмов и программ точечного и интервального оценивания.

Процедура прогнозирования в общем виде сводится к следующим операциям:

1) Выбор класса моделей и получение данных измерений;

2) Решение задачи структурной идентификации (алгоритм решения этой задачи в общем виде показан на рис. 2);

3) Экстраполяция оптимальной по критерию воспроизводимости модели на будущие периоды времени.

4) Определение момента первого выхода прогноза за пороговое значение.

Рассмотрим эти операции применительно к классу решаемых задач.

1. *Выбор класса моделей*. Модели регулярных составляющих исследуемых процессов двух основных видов – в виде степенного полинома.

Поскольку каждый из факторов $\varphi_k(t)$ допускает многократные измерения, можно считать его квазинепрерывной функцией и для его аппроксимации использовать разложения в ряд вида [1], который в данном случае вырождается в степенной ряд. Для решения задач идентификации с заданной точностью ограничимся моделями вида [2]:

$$\varphi_k(t) = a_{k0} + a_{k1}t + a_{k2}t^2 + \ldots + a_{kN}t^N + \varepsilon_k, \qquad (1)$$

где

N — количество членов степенного ряда обеспечивающих точность и устойчивость модели фактора y вариациям данных;

$k = \overline{1,K}$ — условный номер фактора в фактор-модели;

ε_k — ошибка модели или случайная составляющая процесса. И модели [3]

$$\varphi_k(t) = \varepsilon(t) + a_0 + a_1 t + a_2 t^2 + \ldots + a_N t^N + \\ + a_{N+1}\cos(\omega_1 t + \beta_1) + a_{N+2}\cos(\omega_2 t + \beta_2) + \ldots + a_{N+3}\cos(\omega_3 t + \beta_3), \quad (2)$$

где ε_k — нерегулярная (случайная) составляющая наблюдаемого процесса, содержащей гармонические компоненты.

2. *Решение задачи структурной идентификации* (рис. 2). В качестве базового метода для решения этой задачи определен метод максимума компактности.

Во-первых, в качестве метода параметрической идентификации используется метод среднего [1].

Применительно к задаче параметрической идентификации моделей вида (1) алгоритм, реализующий метод среднего сводится к следующим операциям.

1) Для очередной структуры модели

$$(s_{l,1}, s_{l,2}, \ldots, s_{l,N}), \quad \forall l, n : s_{l,n} \in \{0,1\}, \quad n = \overline{1, N}, \quad (3)$$

определяется количество ее свободных параметров:

$$M_l = \sum_{n=1}^{N} s_{l,n}. \quad (4)$$

2) Пробная выборка $Y_{\text{пробн}}(t_k) = Y_k$, $k = \overline{1, K}$ объема K делится последовательно на M_l подвыборок приблизительно одинакового объема. Не снижая в значительной мере общности алгоритмов будем полагать, что все подвыборки имеют одинаковый объем q.

3) Для каждой из подвыборок формулируется требование: модель должна в среднем совпадать с данными подвыборки, что дает систему M_l линейных уравнений с M_l неизвестными:

$$\begin{cases} s_{l,1}b_0 q + s_{l,2}b_1 \sum_{k=1}^{q} t_k + \cdots + s_{l,N}b_N \sum_{k=1}^{q} t_k^N = \sum_{k=1}^{q} y_k \\ s_{l,1}b_0 q + s_{l,2}b_1 \sum_{k=q+1}^{2q} t_k + \cdots + s_{l,N}b_M \sum_{k=q+1}^{2q} t_k^N = \sum_{k=q+1}^{2q} y_k \\ s_{l,1}b_0 q + s_{l,2}b_1 \sum_{k=(M_l-1)q+1}^{qM_l} t_k + \cdots + s_{l,N}b_M \sum_{k=(M_l-1)q+1}^{qM_l} t_k^N = \sum_{k=(M_l-1)q+1}^{qM_l} y_k \end{cases} \quad (2)$$

где b — свободные параметры модели.

Как показано, в [4] оценки метода среднего являются несмещенными и состоятельными. Они уступают по эффективности оценкам метода наименьших квадратов приблизительно в $\sqrt{M_l}$ раз, где M_l — количество свободных параметров модели. Например, для 4-х параметрической модели эти оценки теоретически дают вдвое большую дисперсию погрешности, чем оценки МНК. Вместе с тем, они являются более устойчивыми с вычислительной точки зрения и существенно более робастными – более устойчивыми к отдельным выбросам реализаций случайных процессов. Последнее свойство с учетом особенностей наблюдаемых реализаций является в условиях решаемых задач более важным.

Рис. 2. Общий вид алгоритма структурной идентификации

Система уравнений (5) решается одним из известных методов численного решения систем линейных алгебраических уравнений, например методом исключения с прямым и обратным ходом.

Сделаем ряд замечаний о выборе показателя воспроизводимости Q_l. При обосновании применимости метода максимума компактности рассматривался показатель K_f, основанный на сравнении плотностей распределения ошибок модели на пробной и контрольной выборках.

Наиболее правдоподобному варианту плотности распределения вероятностей $f(X)$ переменной X из числа рассматриваемых вариантов соответствует максимум показателя воспроизводимости:

$$K_f = \int_{-\infty}^{\infty} \inf_f \left\{ f_{\text{пробн}}(x) - f_{\text{контр}}(x) \right\} dx ,$$

где $f_{\text{пробн}}(x)$, $f_{\text{контр}}(x)$ — оценки плотности вероятности по пробной и контрольной выборкам.

Этот показатель имеет некоторые недостатки, применительно к решаемым задачам:

- результаты измерений представляются дискретными рядами. Для дискретных величин понятие плотности распределения, вообще говоря, не определено;
- даже аппроксимация неизвестных распределений в условиях начальной задачи статистики плотностями превращается в существенную проблему.

В настоящей работе предлагается использовать показатели, основанные на сравнении интегральных функций распределения величин. Такие показатели имеют следующие преимущества:

- функцию распределения имеют любые величины – дискретные, непрерывные, комбинированные;
- имеется простая статистика, позволяющая непосредственно по данным измерений $Y_{\text{изм}}(t_k) = Y_k$, $k = \overline{1, N}$ строить эмпирические функции распределения:

$$F_{изм}(y) = \frac{1}{K} \sum_{k=1}^{K} h(y - Y_k), \quad h(y) = \begin{cases} 0, & y < 0 \\ 1, & y \geq 0 \end{cases}. \tag{6}$$

Для сравнения пар функций распределения можно использовать различные метрики [5]. Конкретный показатель Q_l, основанный на квантильной метрике используемой далее.

Для вычисления показателя воспроизводимости по пробной и контрольной выборке одинакового объема *K*, *2K=N*, где *N* — общий объем выборки применяется следующий алгоритм, для модели с номером l вычисляются ее невязки на участках пробной и контрольной выборок:

$$\delta_{l,k}^{\text{пр}} = Y_k - y_l(t_k), \quad k = \overline{1, K}, \tag{7}$$

$$\delta_{l,k}^{\text{конт}} = Y_k - y_l(t_k), \quad k = K+1, K+2, \ldots, 2K . \tag{8}$$

Из полученных выборок невязок (7) и (8) формируются ранжированные выборки, содержащие те же самые числа, но расположенные в порядке возрастания. Далее эти выборки обозначаются так же, как и выборки (7) и (8) с учетом того, что в ранжированных выборках $\delta_{l,k}^{\text{пр,конт}} \leq \delta_{l,k+1}^{\text{пр,конт}}$. Очевидно, что члены ранжированных выборок составляют последовательность квантилей порядка $1/K$ эмпирических распределений. Показатель воспроизводимости вычисляется после этого как средний

модуль отклонения квантилей распределений невязок на пробной и контрольной выборках:

$$Q_l = \frac{1}{K}\sum_{k=1}^{K}\left|\delta_{l,k}^{\text{пр}} - \delta_{l,k}^{\text{конт}}\right|. \qquad (9)$$

Показатель Q_l вычисляется для моделей всевозможных структур и в качестве оптимальной выбирается та из них, для которой он принимает минимальное значение (блок 6 алгоритма рис. 2).

Рассмотрим вычисление показателя (9) для линейной модели. Из табл. 1 следует, что наиболее сложной операцией при вычислении показателя 9 является операция ранжирования выборок. Такая операция выполняется многократным применением алгоритма поиска минимального значения массива чисел и не представляет принципиальных сложностей. В то же время, очевидно, что требованию линейности критериев метода максимума компактности показатель (9) удовлетворяет.

Таблица 1.

Вычисление показателя воспроизводимости для линейной модели

Номер недели, t_k	$Y_{\text{пробн}}(t_k)$	$Y_{\text{контр}}(t_k)$	$Y_1(t_k)$	σ_k	$\sigma_{k\ \text{ранжир}}$	$\left\|\delta_{l,k}^{\text{пр}} - \delta_{l,k}^{\text{конт}}\right\|$
1	29.3		22.9	6.4	-7.1	
2	19.1		26.2	-7.1	-5.1	
3	26.2		29.5	-3.3	-3.3	
4	39.3		32.8	6.5	-1.4	
5	31.0		36.1	-5.1	1.3	
6	42.2		39.4	2.8	2.8	
7	41.4		42.8	-1.4	6.4	
8	47.4		46.1	1.3		
9		50.9	49.4	1.5	-13.6	6.5
10		58.5	52.7	5.8	-6.5	1.4
11		61.6	56.0	5.6	-6.0	2.7
12		53.3	59.3	-6.0	0.3	1.7
13		56.1	62.6	-6.5	1.5	0.2
14		52.3	65.9	-13.6	2.2	0.6
15		71.4	69.2	2.2	5.6	0.8
16		72.8	72.5	0.3	5.8	5.8
Сумма модулей межквантильных отклонений						19.7
Значение показателя воспроизводимости Q						2.5

Для сравнения моделей различных структур аналогичные вычисления показателя Q_l проводятся по тому же алгоритму. Результаты вычислений приведены в табл. 2. Анализ этой таблицы показывает, что модель в виде полинома первой степени является оптимальной по выбранному критерию, что согласуется с физической стороной решаемой задачи.

Отдельную проблему представляет параметрическая идентификация моделей вида (2) с гармоническими составляющими. Даже при известных периодах гармонических составляющих (сутки, неделя, год), соответствующие фазы входят в уравнения нелинейно. Точных методов решения систем нелинейных уравнений не существует, что может приводить к неоднозначности прогнозирования.

Таблица 2.

Значения показателей воспроизводимости для моделей различны структур

№ модели	Вектор структуры			Вид модели	Q
	S_1	S_2	S_3		
1	1	0	0	b_0	7.2
2	0	1	0	$b_1 t$	8.3
3	1	1	0	$b_0 + b_1 t$	2.5
4	0	0	1	$b_2 t^2$	18.6
5	1	0	1	$b_0 + b_2 t^2$	11.3
6	0	1	1	$b_1 + b_2 t^2$	12.7
7	1	1	1	$b_0 + b_1 + b_2 t^2$	8.4

В рассматриваемых случаях, однако, имеется возможность привязки по фазе к характерным особенностям графиков загрузки портов. А именно, в суточных и недельных графиках имеются характерные особенности – час наибольшей нагрузки (ЧНН), день наибольшей нагрузки в неделю (ДНН), час минимальной нагрузки (ЧМН), день минимальной нагрузки (ДМН).

Из графика загрузки одного из портов (рис. 3) магистрального свитча условного провайдера 2 за двое суток видно, что падение загрузки в ЧМН является весьма устойчивым и соответствует примерно 5-6 часам утра.

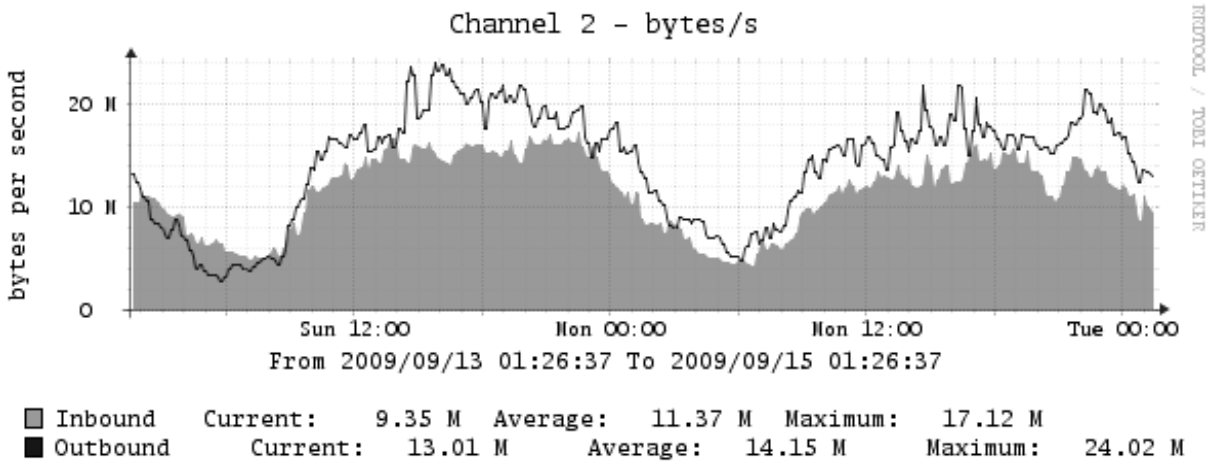


Рис. 3. График загрузки порта 2 условного провайдера за 2 суток

С учетом устойчивости фазы ЧМН применим квазиоптимальный метод ее определения. Как видно суточные колебания нагрузки составляют приблизительно от 40 Мбит/с в ЧМН до 160 Мбит/с в ЧНН. За этот же период линейная долгосрочная составляющая процесса изменения нагрузки изменится приблизительно на 3–30 Мбит/с. На таком коротком временном интервале, таким образом, можно ограничиться простой моделью тренда:

$$y(t) = a_0 + a_1 \cos(\omega_1 t + \beta_1), \tag{10}$$

где ω_1 — известная круговая частота, соответствующая суточному периоду; ее численное значение зависит от единицы измерения времени (секунда, минута, обычно – час).

Поскольку за период сумма отсчетов гармонической составляющей, выполненных через равные интервалы времени, равно нулю, то оценка постоянной составляющей a_0 в зависимости (10) получается так:

$$a_0 = \frac{1}{N}\sum_{n=1}^{N} Y_n \ . \qquad (11)$$

После этого в модели (10) остается 2 свободных параметра – амплитуда суточных колебаний a_1 и фаза β_1. С учетом высокого быстродействия современных компьютеров и невысокой частоты измерений задача определения этих параметром может быть решена комбинированным алгоритмом – полного перебора по фазе и поиска оптимума по амплитуде, а именно:

- осуществляется выбор очередного возможного значения фазы $\beta_{1,k} = t_k$, $k = \overline{1, N}$;
- при заданном значении фазы $\beta_{1,k}$ методом половинного деления или другим быстро сходящимся методом минимизации функции одной переменной осуществляется поиск минимума по a_1 функционала

$$\Phi_k = \sum_{n=1}^{N} \left| a_1 \cos(\omega_1 t_n + \beta_k) - (Y_n - a_0) \right| \xrightarrow[a_1]{} \min \ ; \qquad (12)$$

- в качестве оптимальной выбирается фаза β_k, для которой значение функционала Φ_k минимально.

Для определяются фазы недельной составляющей выполняется идентификация моделей вида (10) для суточных составляющих 1-х, 2-х,..., 7-х суток недели. Фаза выбирается так, чтобы ДНН соответствовал суткам с максимальным значением параметра a_1.

Как видим, после определения фаз модели вида (2) идентификация ее свободных параметров сводится к составлению и решению систем линейных уравнений, аналогичных системе уравнений

$$\omega_i = \omega_i : \left\{ z_i \notin \left[z_{i\min}, z_{i\max} \right] \right\}$$

Таким образом, в настоящей работе рассмотрены алгоритмы идентификации моделей, позволяющие осуществлять точечные прогнозы.

Выводы

В работе рассмотрена общая методика прогнозирующего контроля современных мультисервисных сетей. Эта методика в качестве основного компонента включает алгоритмы структурной идентификации моделей регулярных составляющих (трендов) наблюдаемых процессов. Полученные результаты позволяют сформулировать ряд выводов.

1) Предложенный для решения задач параметрической идентификации метод среднего доставляет устойчивые с вычислительной точки зрения и робастные оценки.

2) Предложенный показатель воспроизводимости моделей по данным контрольной выборки удобен с вычислительной точки зрения и не требует априорного знания законов распределения наблюдаемых величин.

3) В зависимостях наблюдаемых факторов, влияющих на отказоустойчивость, имеются выраженные периодичности. Для решения задач идентификации целесообразно применять квазиоптимальные методы решения нелинейных уравнений, когда неизвестная фаза определяется по характерным точкам. При этом общая задача декомпозируется на подзадачу определения фазы гармонической составляющей и последующему решению системы линейных уравнений.

Список литературы

1. Волков, Е.А. Численные методы [Текст] : учеб. пособие [для инж.-техн. спец. вузов] / Е.А. Волков. — Изд. 5-е, стер. — СПб. : Лань, 2008. — 248 с.
2. Казакова, Н.Ф. Анализ принципиальной задачи факторизации модели отказа предоставления услуги в сети NGN на уровне управления сетью / Н.Ф. Казакова, В.И. Гура // Інформаційна безпека. — 2010. — № 1(3). — С. 127–130.
3. Сергеев, В.В. Процедура получения функций изменения факторов, влияющих на качество предоставления услуг в мультисервисных сетях / В.В. Сергеев, А.М. Мухин // Інформаційна безпека. — 2010. — № 2(4). — С. 139–145.
4. Альтшуллер, Г.С. Найти идею [Текст] : введ. в теорию решения изобрет. задач / Г.С. Альтшуллер; отв.ред. А.К. Дюнин; АН СССР, Сиб. отд-ние. — 2-е изд., доп. — Новосибирск : Наука. Сиб. отд-ние, 1991. — 223 с.
5. Робастность в статистике [Текст] : поход на основе функций влияния / Ф. Хампель, Э. Рончетти [и др.] ; пер. с англ. под ред. В.М. Золотарева. — М. : Мир, 1989. — 512 с.

АЛГОРИТМ ТОЧКОВОГО ПРОГНОЗУВАННЯ ВИПАДКОВИХ ПРОЦЕСІВ В АВІАЦІЙНИХ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Д.В. Чирков, В.Г. Ліповський

Національний авіаційний університет,
просп. Космонавта Комарова, 1, Київ, 03680, Україна

У роботі розглянута загальна методика прогнозуючого контролю сучасних мультисервісних мереж, яка в якості основного компоненту включає алгоритми структурної ідентифікації моделей регулярних складових (трендів) процесів. Наведена загальна структура методики прогнозуючого контролю авіаційних інфокомунікаційних систем. Представлений загальний вигляд алгоритму структурної ідентифікації.

Ключові слова: інфокомунікаційні мережі, авіаційні мережі, випадкові процеси, точкове прогнозування, алгоритм прогнозування, мультисервісні мережі

POINT PREDICTION ALGORITHM FOR STOCHASTIC PROCESSES IN AIRCRAFT COMMUNICATION NETWORKS

Dmytro V. Chirkov, Valery G. Lipovsky

National Aviation University,
1 Kosmonavta Komarova Ave., Kyiv, 03680, Ukraine

The paper focuses on general method of predictive control of modern multi-service networks, which is a major component includes algorithms for the identification of structural models of regular components (trends) of the observed processes. The general structure for predictive control of aircraft communication systems is described. The general view of the structural identification algorithm is discussed.

Keywords: information and communication networks, airline networks, stochastic processes, point forecasting, prediction algorithm, multi-service networks

УДК 004.056

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 2, pp. 123-131

МОДЕЛЬ ФОРМУВАННЯ ДЕРЕВА АТАК ДЛЯ ОДЕРЖАННЯ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ І МЕРЕЖАХ ПРИ ВИЛУЧЕНОМУ ДОСТУПІ

В.Л. Бурячок

Військова частина А1906,
Україна; e-mail: bur@ukr.net

У статті, зважаючи на низку проблем, пов'язаних із забезпеченням продуктивності, надійності та стійкості функціонування інформаційно-телекомунікаційних систем, а також можливості несанкціонованого доступу до циркулюючих у таких системах інформаційних ресурсів, розглянуто один із можливих методів одержання інформації за рахунок формування дерева атак при вилученому доступі.

Ключові слова: інформація, дерево атак, інформаційно-телекомунікаційна система, інформаційно-комунікаційні технології, об'єкти інформаційної діяльності, несанкціонований доступ

Вступ

Наприкінці XX – початку XXI сторіччя завдяки глибоким системним перетворенням, викликаним синтезом перспективних інформаційно-комунікаційних технологій (ІКТ) та бурхливим розвитком інформаційно-телекомунікаційних (ІТ) систем і мереж у світі та Україні зокрема суттєво активізувалась робота за напрямами:

- виявлення інформаційних потреб та добору джерел інформації;
- пошуку та збору інформації у відкритих і відносно-відкритих, а також її добування із закритих електронних джерел;
- опрацювання інформації, оцінювання її повноти і значущості;
- подання інформації у зручному для користувачів вигляді та організації зворотного зв'язку з нею;
- використання інформації для оцінювання тенденцій, розробки прогнозів, оцінювання альтернатив рішень і дій, вироблення стратегій тощо.

Цьому сприяло створення спеціальних ІТ систем (СІТС), що мали високі споживчі якості та були здатні реалізовувати певні обчислювальні, відслідковувальні, запам'ятовувальні, комунікаційні, інформаційні, регулювальні, оптимізаційні, прогнозні, аналітичні та документувальні функції, зростання кількості та висока технологічність нових засобів і методів деструктивного впливу протиборчими сторонами на об'єкти інформаційної діяльності (ОІД) один одного, підвищення професіоналізму потенціальних порушників тощо.

Зважаючи на те, що масштаби застосування сучасних ІКТ останнім часом розширились до практично неосяжних меж поряд із проблемами забезпечення продуктивності, надійності та стійкості функціонування ІТС (СІТС) це визначило також й проблему несанкціонованого доступу (НСД) до циркулюючих у таких системах інформаційних ресурсів (ІР). З одного боку ця проблема нині обумовлюється, як відомо, посиленою увагою до безпеки ІТС (СІТС), а з іншого – неухильно

зростаючими збитками, які порушники завдають власникам ІР. Вирішити її, як показує статистика, можна за рахунок використання існуючих та розроблення нових методів і засобів несанкціонованого отримання інформації з таких систем.

Аналіз останніх досліджень і публікацій

Зазначене завдання у певних аспектах висвітлено в публікаціях як зарубіжних, так і вітчизняних авторів. Найвідомішими серед них є роботи А.В. Возженікова, В.І. Ярочкіна, Г. Почепцова, М. Лібіцкі, К.А. Мініхена, О. Шермана, Ф. Фукуями та інших фахівців. Проте аналіз цих та багатьох інших джерел свідчить, що комплексного оцінювання палітри методів і засобів несанкціонованого одержання інформації із СІТС до цього часу, нажаль, не проводилось. Зважаючи на те, що вирішення цього завдання достатньо суттєво залежить від використовуваної операційної системи (ОС), систем управління базами даних (СУБД) та мережевого програмного забезпечення (МПЗ), параметрів безпеки, а також інших факторів, воно потребує додаткового і більш глибокого вивчення.

Отже, актуальність статті зумовлено передусім обсягом інформації, що останнім часом надходить до користувачів із зовнішнього середовища та безперервно зростає, а також потребою підвищення вимог до захисту такої інформації від НСД. Важливою умовою розв'язання сформульованих вище проблем стає оперування єдиним понятійним апаратом у цій царині та знання специфіки процесів злому ІТ систем потенційними порушниками. Тому *мета* статті та її основний зміст саме й полягають у викладенні можливого варіанту (алгоритму) дій хакерів (крекерів тощо) щодо формування дерева атак для отримання доступу до спеціальних ІТС протиборчої сторони, тобто їх злому.

Виклад основного матеріалу

Враховуючи, що загальне програмне забезпечення будь-якої ІТС або СІТС складається з трьох основних компонент – ОС, СУБД та МПЗ [1], варіант несанкціонованого одержання інформації шляхом злому систем захисту цих компонент при вилученому доступі може бути поданий структурно-логічною схемою, наведеною на рисунку 1 [2].

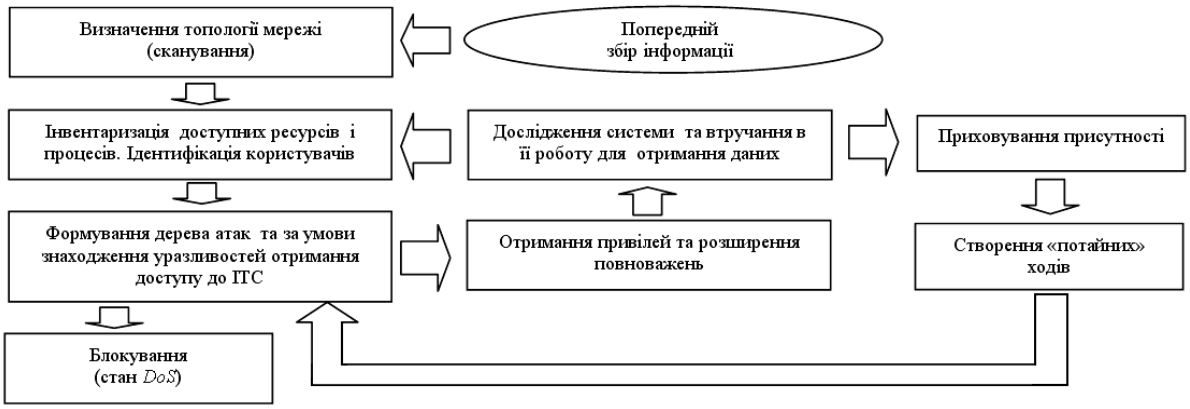


Рис. 1. Структурно-логічна схема методу несанкціонованого одержання інформації з ІТС (СІТС)

Головними дійовими особами цього процесу виступають внутрішні поодинокі інсайдери, або зовнішні організовані злочинні співтовариства – кіберугруповання хакерів (комп'ютерних професіоналів високого рівня, які в ході проникнення до СІТС жертви не здійснюють протиправних дій) і крекерів (хакерів, які застосовують свої знання для злому КМ явно з корисною метою), а також терористичні і розвідувальні організації, дії яких розгортаються як правило за таким типовим алгоритмом. *На першому кроці* порушниками проводиться так звана пасивна розвідка шляхом:

1) пошуку інформації про об'єкт розвідки та збору інформації про нього. Для цього порушники використовують відомі пошукові системи та/або спеціалізовані пошукові машини й працюють з відкритими джерелами в Internet, а саме: адресами й місцями розташування офісів на web-вузлах; інформацією про ділових партнерах; номерами телефонів та електронною поштою тощо. При цьому вони, як правило, ставлять собі за мету одержати відповіді на такі питання:

- ім'я домену або доменів об'єкта розвідки;
- адреси підмереж, якими він володіє;
- точні адреси вузлів, що знаходяться на периметрі мережі об'єкта розвідки та їх ролі;
- механізми мережної безпеки, використовувані об'єктом розвідки (міжмережні екрани, фільтруючі маршрутизатори, системи виявлення атак);
- сервіси та ОС, запущені на визначених вище вузлах, тощо.

Окрім цього порушники можуть збирати щодо об'єкта розвідки відомості про SNMP, таблиці маршрутизації та інші інформаційні і розвідувальні матеріали (відомості, дані);

2) зондування ІТС, тобто визначення комп'ютерів (ПЕОМ), підключених у цей момент до мережі Internet та прослуховування мережного трафіку. Ці операції порушники здійснюють з використанням *Traseroute*, *VisualRoute*, *NeoTrace* та інших ним подібних програм.

Запобігти діям порушників у проведенні пасивної розвідки допоможуть правильно налаштовані програмно-апаратні засоби виявлення вторгнень, а саме: маршрутизатори і брандмауери, а також програмні файєрволи.

Другим кроком дій порушників є активна розвідка, що передбачає:

- сканування мережі, тобто визначення її топології, з використанням *ping*-подібних утиліт. Кращими з них вважаються *Nmap*, *Ping Sweep* виробництва компанії *Solar Winds* та інші ним подібні програмні додатки;
- визначення відкритих портів у системі – тобто, точок входу в систему, установлених різними додатками й процесами, що очікують підключення. Для цих цілей порушниками використовуються, як правило, утиліти типу *Nmap*, *Super Scan*, *IP Eye*, *NetCat*, тощо;
- інвентаризацію користувальницьких ресурсів і облікових записів. Ці операції порушники можуть робити скориставшись *Win2K Resource Kit*, а також убудованими командами системи, такими як *net view*, *nbtstat* та ним подібними.

Запобігти діям порушників у проведенні активної розвідки допоможуть правильно й жорстко налаштовані списки на брандмауерах, обмеження доступу до відкритих портів, а також внесення змін у визначенні значення в реєстрі ОС.

Далі, *на третьому кроці*, якщо знайдені уразливості в СІТС жертви й таким чином отриманий доступ до неї, порушниками здійснюється сукупність заходів, що мають за мету саме зламування системи. Вони реалізуються шляхом:

- формування дерева атак (F_{atak});
- зламування та/або неправильного налаштування наявного ПЗ;
- використання сценаріїв автоматизації;
- розширення повноважень, тощо.

З метою ефективної реалізації процедури формування дерева атак її формалізована модель, з урахуванням пропозицій [3–6], може бути представлена кортежем (рис. 2):

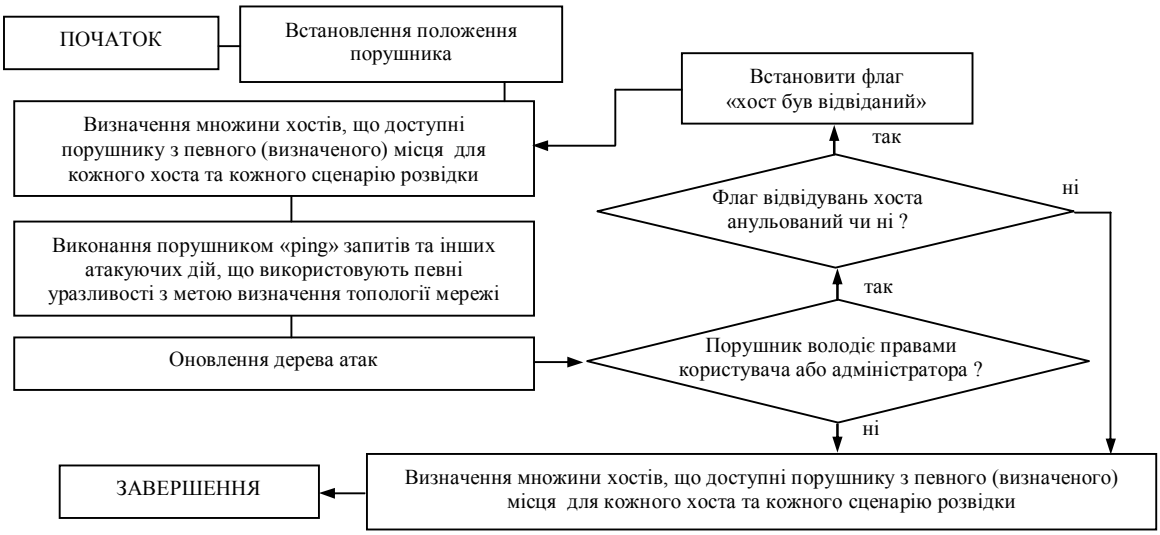


Рис. 2. Алгоритм формування дерева атак для визначеного положення порушника

$$F_{АД} = \left\langle M_{АД}^{об'єкт}, M_{АД}^{сценарій}, M_{АД}^{варіант} \right\rangle, \qquad (1)$$

де

$M_{АД}^{об'єкт}$ — компонент, що описує параметри процесу аналізу захищеності (АЗ), а саме рівень атакуючих дій і програмний код за рахунок якого ці дії можуть бути реалізованими та який визначає множину аналізованих об'єктів, мету виконання атакуючих дій, що може являти собою, наприклад, пару «об'єкт атаки – мета атаки» (наприклад, хост Workstation, «сканування портів») та параметри, що характеризують порушника $M_{П} = F\left(K_{пристр}^{мер}, K_{ОС+серв}^{відомі}, p_{поруш}^{положж}\right)$, де $K_{пристр}^{мер}$ — множина пристроїв у мережі; $K_{ОС+серв}^{відомі}$ — множина відомих порушнику ОС і сервісів; $p_{поруш}^{положж}$ — початкове положення порушника у мережі ($p_{поруш}^{положж} \in K_{пристр}^{мер}$);

$M_{АД}^{сценарій}$ — компонент, що описує сценарний рівень (рис. 3) й слугує для формування множини послідовності атакуючих дій з урахуванням мети, сформованої на рівні параметризації процесу АЗ, що повинна бути досягнута порушником. Формування сценаріїв атак здійснюється шляхом визначення та повного перебору всіх підцілей атакуючих дій цілі T (наприклад, ціль T – «розвідка», підцілі – «сканування портів», «визначення типу ОС», тощо);

$M_{АД}^{варіант}$ — компонент, що описує всі можливі варіанти виконання атакуючих дій порушником з урахуванням їх характеристик.

При цьому кожна з підцілей може бути коренем (вершиною) власного дерева атак і мати власний атрибут, наприклад, тривалість життя (визначає тривалість подій для цілей і підцілей), степінь конфіденційності (визначає імовірність досягнення цілі, якщо мета підцілі досягнута) тощо. За таких умов, наприклад, коренем (вершиною) дерева атак «Bypassing 802.1x» (рис. 4) може бути ціль T , що має за мету «Обхід 802.1x» [5].

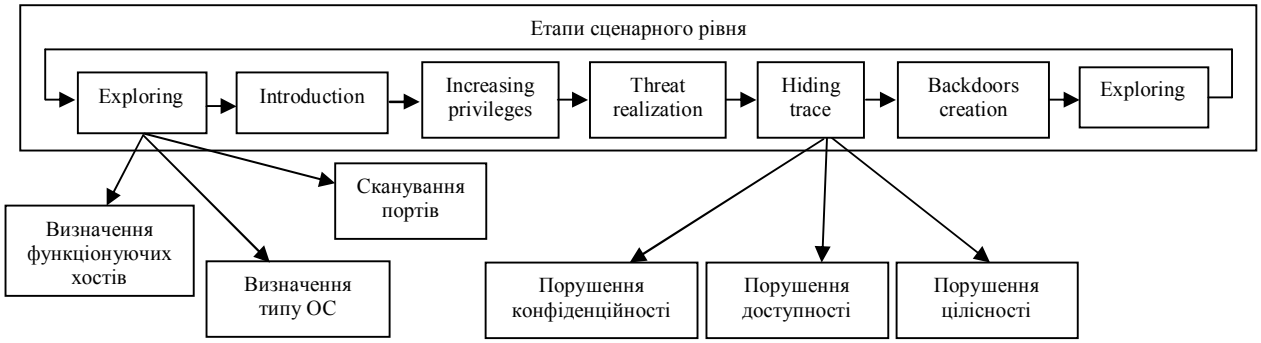


Рис 3. Фрагмент сценарного рівня з узагальненої моделі атак

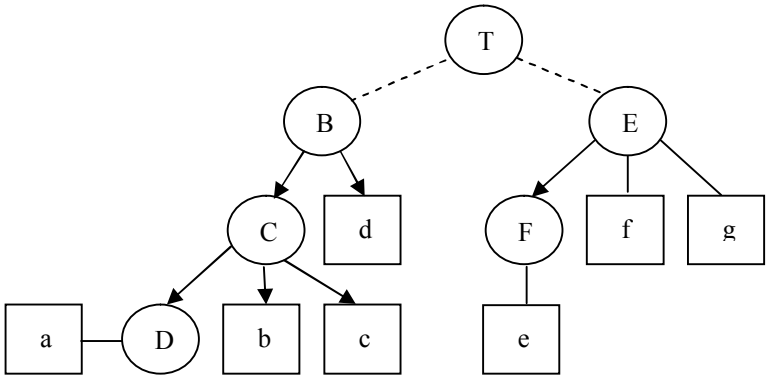


Рис. 4. Дерево атаки «Bypassing 802.1x»

Для її реалізації необхідно «Перехопити сеанс автентифікації 802.1x» (підціль B) або провести атаку «Людина посередині у сеансі 802.1x» (підціль E). Підціль B у свою чергу може бути досягнута за рахунок досягнення або підцілі C – «Відключення клієнта» (реалізувати яку, наприклад, для мережі WLAN можна виконавши атаки типу «Підміна АР» (підціль D), «Підслуховування MAC-адреси точки доступу» (підціль b), або «Відправлення повідомлення про відключення MAC-адреси» (підціль c)), або підцілі d – «Підміна автентифікованого клієнта 802.1x», тощо.

Підціль E у свою чергу може бути досягнута за рахунок підбору пароля або ж шляхом використання злоякісного (шпигунського) ПЗ і методів соціальної інженерії. Атрибути, що притаманні підцілям наведені у табл. 1.

Тобто, дане дерево має два можливі шляхи атаки, що означає два сценарії атаки для досягнення поставленої мети:

$$T\left(B\left(C\left(D\left(a\right),b,c\right),d\right)\right) \text{ та } T\left(E\left(F\left(e\right),f,g\right)\right).$$

З урахуванням пропозицій [4–6] компонент $M_{АД}^{варіант}$ може бути представлений таким кортежем:

$$M_{АД}^{варіант} = F\left(A, E, F^{АД}\right),$$

де

$A = \left\{U_i^{зовн}, U_i^{внутр}\right\}_{i=1}^{N_A}$ — множина всіх атакуючих дій N_A (являє собою сукупність внутрішніх $U^{внутр} = \left\langle S_m^{вн}, K, З^{безп}, П, O^k\left(C_m^k\right)\right\rangle$ і зовнішніх $U^{зовн} = \left\langle S_m^{зв}, K, З^{безп}, П, O^k\left(C_m^k\right)\right\rangle$

атак на СІТС, що використовують уразливості як програмних, так і технічних засобів системи);

$S^{зв}$ — зовнішнє джерело загрози;

$S^{вн}$ — внутрішнє джерело загрози;

K — комунікаційне обладнання у каналі зв'язку;

$З^{безп}$ — мережеві, хостові, параметричні сервіси безпеки на шляху розповсюдження атаки;

$П$ — протоколи; пакети;

O^k — об'єкт доступу;

C_m^k — сегмент СІТС, у якому обробляється інформація й найвищий рівень критичності якої дорівнює k;

m — номер сегменту;

$E = \{e_i\}_{i=1}^{N_e}$ — множина всіх вірусів (програмних кодів, виконання яких дасть можливість порушнику реалізувати атакуючу дію);

$F^{АД}$ — множина функцій даного компонента (складається з функції, яка дає можливість порушнику повернутися до виконання атакових дій, якщо поставлена ним мета не досягнута та функції, яка веде облік знань і умінь порушника, тобто, здатна з множини усіх атакових дій видалити ті, що в умовах свого виконання містять невідомі йому ОС та сервіси).

Таблиця 1.

Архітектура мережі та призначення її складових елементів

Підцілі	Сценарії атак	Атрибути тривалості життя
B	$T(B(C(D(a),b,c),d))$	4/4=1
C	$T(B(C(D(a),b,c),d))$	3/4=0.75
D	$T(B(C(D(a),b,c),d))$	1/4=0.25
E	$T(E(F(e),f,g))$	3/3=1
F	$T(E(F(e),f,g))$	1/3=0.33

Наповнення множин A та E, згідно [4] має здійснюватися на основі відкритих БД уразливостей, наприклад, Open Source Vulnerability Database або National Vulnerability Database (NVD), а також експертних знань (атакуючі дії етапів впровадження, підвищення привілеїв і реалізації загрози, пасивної і активної розвідки, приховування слідів, створення потайних ходів тощо). За таких обставин кожна атакуюча дія складатиметься з: високорівневого ідентифікатора; мети, що досягається виконанням даних дій; множини умов виконуваності; подання впливу на об'єкт, що атакується (послідовність мережевих пакетів, команд ОС, вірусів або експлойтів); множини результатів атакуючих дій; множини рекомендацій з усунення уразливостей.

Таким чином, наявність моделі формування дерева атак при реалізації власних процедур віддаленого доступу до ІТ і криптосистем протиборчої сторони дасть можливість: підвищити ймовірність подолання неавторизованим користувачем засобів захисту СІТС від вірусних атак та несанкціонованого одержання інформації з їх основних компонент таких, як ОС, СУБД та МПЗ; описати всі можливі варіанти виконання порушником атакуючих дій з урахуванням їх характеристик, представивши при цьому корінь дерева атак трійкою одиниць виду: «Стан СІТС на момент реалізації

АД, Атакуюча дія, Об'єкт АД». Оцінити рівень її складності можна з такого відомого виразу [4]:

$$F_{atak}(H_V) \le \begin{cases} K_{yrazl} \sum_{i=1}^{H_V-1} A_{\max}^{(i-1)} \frac{H_V!}{(H_V-i)!} \text{ при } H_V = H \\ K_{yrazl}\left[H \sum_{i=0}^{H_V-1} A_{\max}^{(i)} \frac{H_V!}{(H_V-i)!} + \sum_{i=1}^{H_V-1} A_{\max}^{(i-1)} \frac{H_V!}{(H_V-i)!} \right] \text{ при } H_V \ne H \end{cases} \quad (2)$$

де

H — множина аналізованих хостів у СІТС ($H = |K_H|$ — число хостів);

K_{yrazl} — число уразливостей у внутрішній базі даних;

$H_V \subset H$ — множина хостів у СІТС, що мають уразливості та дають можливість порушникові отримати права користувача або адміністратора ($H_V = |K_{H_V}|$ — число даних хостів);

A_{h_V} — кількість уразливостей на хості $h \in H_V$, що дають можливість порушникові отримати права користувача або адміністратора й перейти на даний хост ($A_{\max} = \max_{h \in H_V} A_{h_V}$ — максимальне число даних уразливостей по усім хостам аналізованої СІТС).

У подальшому з метою закріплення і розширення своїх привілей (повноважень) порушники можуть використати такі утиліти:

- реєстратори натискань клавіш – *Invisible Key Logger Stealth* (IKS);
- аналізатори мережевих пакетів – сніфери типу *BUTTSniffer*, *NetXRay*;
- утиліти перенацілювання портів *fpipe*, тощо.

Захистом від розширення повноважень на третьому кроці злому СІТС є застосування регулярно оновлюваних антивірусних пакетів, а також використання програм підраховування контрольних сум файлів.

На четвертому кроці завантажується шкідливе програмне забезпечення, результатом роботи якого має бути несанкціоноване отримання даних. При цьому з метою приховування своєї присутності порушники залишають так звані «потайні ходи», застосовуючи для цього, наприклад, такі команди ОС, як *attrib +h*, утиліти *Win2K Resource Kit*, набори «відмичок» – *rootkit* і програму *eLiTeWrap*.

На наступному, *п'ятому кроці* відбувається збереження результатів доступу. З цією метою порушниками застосовуються так звані «люки» (механізми усередині ОС або іншого ПЗ, що дають можливість їх програмам одержати привілейовану функцію або режим роботи, які не були їм дозволені) та програмне забезпечення типу «троянський кінь».

При цьому для вилученого адміністрування та об'єднання можливостей декількох програм з метою асинхронного й прихованого виконання певних деструктивних дій порушниками можуть бути використані так звані троянські коні типу *Net Bus*, *Sub Seven* та *Back Orifice*, а також методи тунелювання (DNS, HTTP, SNMP).

Захистом від дій порушників по несанкціонованому отриманню даних та подальшого збереження ними результатів доступу на четвертому і п'ятому кроках алгоритму може бути застосування програм, що підраховують контрольні суми файлів, відслідковують ведення журналів реєстрації подій та періодичність оновлювання антивірусних баз і системи у цілому.

Останнім кроком зловмисних дій порушників є замітання або інакше знищення ознак їх перебування в системі. Для цього порушники перезавантажують систему шляхом її «бомбардування» пакетами ICMP (*Smarf*-атака) або UDP (*Fraggle*-атака) з використанням посилюючої мережі й переводять її у стан DoS (*Denial of Service*).

Захистом від таких дій може бути встановлення фільтрів у програмно-апаратних файєрволах.

Висновок

Об’єктивною реальністю сьогодення є широке впровадження у сфери життєдіяльності особи, суспільства та держави у цілому сучасних ІКТ, розгортання на їх основі локальних і глобальних ІТС та мереж, об’єднання яких уже сьогодні складає основу нової інфраструктури планети – інфосфери. В Україні, нажаль, має місце низка проблем законодавчого і технічного характеру, які не дозволяють отримати всі переваги від розвитку ІКТ та впровадження ІТС, а інколи і перешкоджають таким процесам або призводять до неефективного використання засобів на їх розробку, впровадження і захист. До найбільш значущих серед них слід віднести:

- фактичну самоізоляцію України від міжнародного інформаційного співтовариства зважаючи на невідповідність законодавства і стандартів нашої держави світовим вимогам;
- відсутність сумісності між ІТС різних відомств і організацій України, що призводить до надмірності у зборі первинної інформації, подорожчання розробок і експлуатації таких систем;
- відсутність централізованої державної структури, що регламентує інформаційні процеси у нашому суспільстві тощо.

Дані проблеми суттєво впливають на створення комплексної системи захисту інформаційного і кіберпросторів України від внутрішніх і зовнішніх злочин і загроз, а також на можливість інтеграції нашої держави у світову інформаційну спільноту.

Список літератури

1. Анин, Б.Ю. Защита компьютерной информации [Текст] / Б.Ю. Анин. — Санкт-Петербург : БХВ, 2000. — 384 с.
2. Бурячок, В.Л. Варіант механізму злому інформаційно-телекомунікаційних систем та їх захисту від стороннього кібернетичного впливу / В.Л. Бурячок // Сучасний захист інформації. — 2011. — № 4. — С. 77–86.
3. Бурячок, В.Л. Основи формування державної системи кібернетичної безпеки [Текст] : монографія / В.Л. Бурячок. — К. : НАУ, 2013. — 432 с.
4. Котенко, И.В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак [Текст] / И.В. Котенко, М.В. Степашкин // Труды Института системного анализа Российской академии наук. — 2008. — Т. 31. — С. 126–207.
5. Машкина, И.В. Управление и принятие решений в системах защиты информации [Текст] : учеб. пособие / И.В. Машкина. — Уфа : УГАТУ, 2007. — 160 с.
6. Степашкин, М.В. Оценка уровня защищенности компьютерных сетей на основе построения графа атак / И.В. Котенко, М.В. Степашкин, В.С. Богданов // Труды международной научной школы «Моделирование и анализ безопасности и риска в сложных системах (МАБР–2006)». — СПб., 2006. — С. 150–154.

МОДЕЛЬ ФОРМИРОВАНИЯ ДЕРЕВА АТАК ДЛЯ ПОЛУЧЕНИЯ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ ПРИ УДАЛЕННОМ ДОСТУПЕ

В.Л. Бурячок

Военная часть А1906,
Украина; e-mail: bur@ukr.net

В статье, учитывая ряд проблем, связанных с обеспечением производительности, надежности и устойчивости функционирования информационно-телекоммуникационных систем, а также возможности несанкционированного доступа к циркулирующим в таких системах информационным ресурсам, рассмотрен один из возможных методов получения информации за счет формирования древа атак при удаленном доступе.
Ключевые слова: информация, дерево атак, информационно-телекоммуникационная система, информационно-коммуникационные технологии, объекты информационной деятельности, несанкционированный доступ

TREE ATTACKS FORMATION MODEL FOR REMOTELY ACCESS TO DATA IN INFORMATION AND COMMUNICATION SYSTEMS AND NETWORKS

Volodymyr L. Buryachok

A1906 Military Unit,
Ukraine; e-mail: bur@ukr.net

This article focuses on one of possible method for remotely access based on formation of tree attacks. Number of problems associated with the performance, reliability and sustainability of information and telecommunication systems, as well as the possibility of unauthorized access to such systems and circulating information resources are described.
Keywords: information, attack tree, information and telecommunication systems, information and communication technologies, information activity, unauthorized access

УДК 519.248

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 2, pp. 132-145

ЭФФЕКТИВНОЕ ПРИМЕНЕНИЕ МАТЕМАТИКО-СТАТИСТИЧЕСКИХ МЕТОДОВ

Е.Л. Даниленко

Одесский национальный политехнический университет
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: sankirillo@yahoo.com

Предлагаются примеры эффективного использования простых математико-статистических методов в промышленном и строительном производстве.

Ключевые слова: статистические оценки, балльные оценки, статистический контроль качества, контрольные карты, однородность гранулометрического состава, качество бетона

Введение

Математико-статистические методы широко развились в 20 веке [1–24], благодаря научно-техническому прогрессу и промышленному производству. Задачи оценки надёжности и контроля качества стимулировали создания научных школ, основателями которых стали выдающиеся математики и мыслители современности А.Н. Колмогоров, Ю.В. Прохоров, Б.В. Гнеденко, В.В. Налимов, Л.Н. Большев, Н.В. Смирнов, В.И. Романовский и их ученики [4–6, 15–29]. За короткий период в Советском Союзе были созданы теория статистических оценок, математическая теория надёжности, теория статистического контроля качества, математическая теория эксперимента [30–43]. Конечно следует отметить, что важное влияние оказало развитие прикладных математико-статистических методов в США, например, по подсчетам профессора Фримена из Массачусетского технологического института [17] только статистический приемочный контроль давал промышленности США более 20 миллиардов долларов в ценах 2001 года, то есть 0.8% валового внутреннего продукта.

В настоящее время статистическая обработка данных проводится, как правило, с помощью соответствующих программных продуктов [44].

В статье показано как простые методы математико-статистического моделирования позволяют решать актуальные задачи промышленного и строительного производства [45–52].

Балльные оценки при контроле технологических процессов

Действенное управление технологическими процессами предусматривает организацию на производстве системы оперативного контроля различных показателей этих процессов. Инструментом такого контроля могут быть контрольные карты [33, 40], позволяющие в графической форме отразить как характер протекания процесса, так и результаты воздействия управляющих факторов. В контрольных картах отражаются и статистические параметры измеримых показателей и количественные характеристики неизмеримых показателей.

Известно, что на ряде производств возможна лишь визуальная оценка качества протекания технологического процесса и уровня готовой продукции. Часто визуальная

оценка используется и там, где инструментальное определение качества хотя и возможно, но сложно и требует дорогостоящей аппаратуры.

В таких случаях результаты контроля удобно формализовать с помощью балльных оценок. Это позволяет в дальнейшем оперировать с результатами контроля как с измеримыми показателями, в частности – использовать их для ведения контрольных карт.

Система баллов для оценки качества технологического процесса разрабатывается на основе анкетного опроса большого числа специалистов (конечно, если она не определена тем или иным нормативным документом). Желательно, чтобы специалисты были из нескольких коллективов – это позволит исключить ошибку в мнениях, вызванную сложившимся в данном коллективе устойчивым представлением о технологическом процессе.

Вопросы анкеты должны давать достаточно полное и всестороннее освещение контролируемого процесса, например: число баллов, присваиваемое каждому контролируемому элементу процесса в момент контроля; периодичность контроля; число баллов, соответствующее отличной, хорошей, удовлетворительной и неудовлетворительной работе отдельных технологических узлов (участков, цехов и т.п.) и процесса в целом за определенные периоды – смену, сутки, декаду, месяц, квартал, год. Максимальное число баллов устанавливается в зависимости от конкретных условий протекания данного технологического процесса (от числа вариантов уровней качества, от числа и степени существенности возможных нарушений технологического регламента и т. д.).

Для оценки качества работы используются средние арифметические баллов, вычисленных по всем анкетам. Этот результат, однако, можно считать надежным лишь при достаточно высокой согласованности мнений как внутри каждого коллектива, так и между коллективами.

Согласованность мнений внутри коллектива выясняется с помощью коэффициента конкордации Кенделла [18, 47]. Согласованность в мнениях между специалистами различных коллективов можно оценить парным сравнением. Для двух коллективов согласованность оценивается с помощью коэффициента ранговой корреляции Спирмена [18, 47].

Обработанные таким способом результаты анкетного опроса можно использовать для организации системы оперативного контроля качества технологического процесса. На контрольные карты следует периодически наносить суммы баллов, характеризующие качество процесса за контролируемый период или уровень нарушений технологического регламента. Суммы складываются из баллов, назначаемых контрольной службой в моменты контроля отдельных элементов процесса. Нанесенные на карты контрольные границы соответствующие отличному, хорошему, удовлетворительному и неудовлетворительному качеству, дают наглядное представление о качестве работы на каждом технологическом узле (производственном участке, в цехе и т.д.). Периодичность нанесения баллов на контрольные карты определяется руководителем, который принимает те или иные решения на основе анализа контрольной карты.

На рис. 1 показана контрольная карта с суммами штрафных баллов, присваиваемых контрольной службой управления строительства Усть-Илимской ГЭС за нарушения технологического регламента на бетонном заводе каждую рабочую смену. В основном качество работы на заводе оценивается как хорошее или удовлетворительное. В отдельные смены (5, 6, 10 и 26 января) качество работы было признано неудовлетворительным, что потребовало принятия срочных мер.

Для анализа причин снижения качества технологического процесса удобно использовать диаграммы Парето [47, 48, 51, 52] которые показывают (рис. 2) как индивидуальные (в виде столбиковой диаграммы), так и суммарные нарушения (в виде кумулятивной кривой). Кумулятивная кривая отчетливо выявляет те элементы техно-

логического процесса, которые больше всего снижают качество. Именно на эти элементы и следует воздействовать с помощью наладки оборудования, его модернизации, обучения персонала и т.д. На рис. 2 видно, что 82.7% от общей суммы штрафных баллов, назначенных за нарушения технологического регламента, дает только один технологический узел (№ 1). Ясно, что именно этот узел и требует первоочередного внимания руководства.

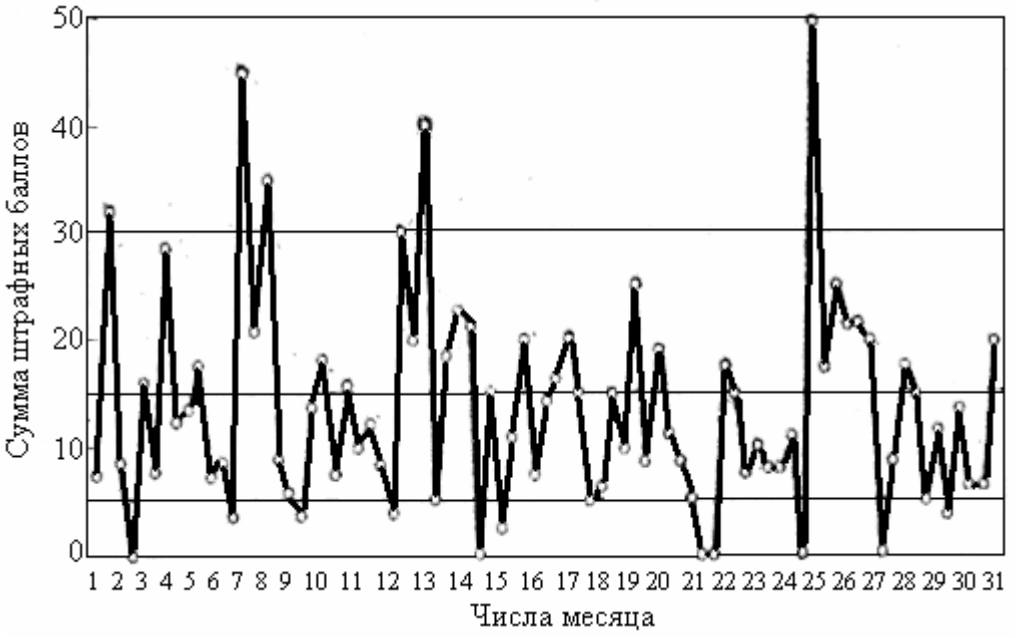


Рис. 1. Контрольная карта суммы штрафных баллов

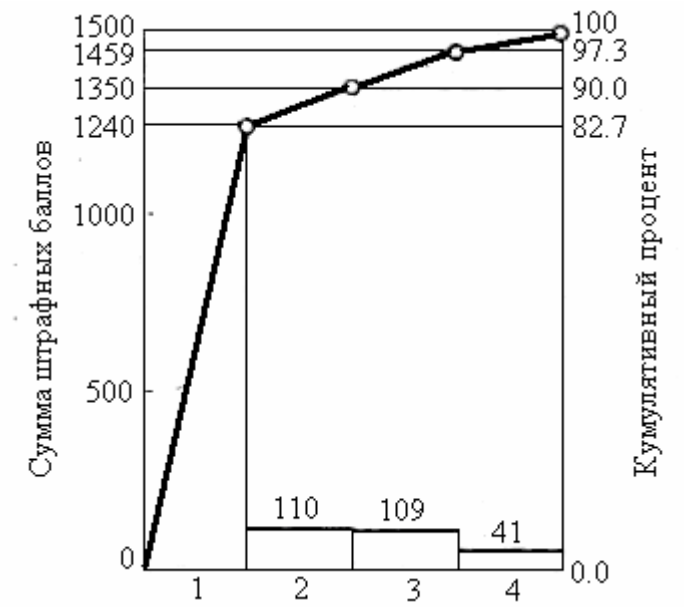


Рис. 2. Диаграмма Парето для суммы штрафных баллов за качество работы: 1 – отделение дозаторное и бетоносмесительное; 2 – отделение транспортеров; 3 – узел контрольного грохочения, 3 – подогрев, 4 – приёмная площадка

Метод балльных оценок был использован для организации системы контроля и управления различными технологическими узлами при строительстве Усть-Илимской ГЭС [48, 51], так как большинство видов нарушения технологических процессов производства и укладки гидротехнического бетона не поддается непосредственной количественной оценке.

Для построения системы был проведен анкетный опрос большой группы специалистов из различных подразделений строительства. Вычисленные на основе анкетных данных коэффициенты конкордации Кенделла и коэффициенты ранговой корреляции Спирмена оказались значимыми (при доверительной вероятности $p = 0.99$) для всех рассматриваемых технологических процессов строительства.

Построенный на основе системы балльных оценок оперативный контроль осуществлялся с помощью контрольных карт. Данные наносились на карты один раз в смену, сутки или месяц – в зависимости от назначения этих карт. Получаемые в результате контроля балльные оценки работы использовались для материального стимулирования работников.

Статистический контроль качества на строительстве Усть-Илимской ГЭС

Усть-Илимская гидроэлектростанция – одна из крупнейших мировых гидроэлектростанций, расположена на реке Ангара в Иркутской области, в городе Усть-Илимск. Строительство ГЭС началось в 1963, закончилось в 1980. Весь этот период действовала система контроля и управления качеством.

Основные принципы системы – оперативность и действенность обеспечиваются методическими приемами контроля, организационными и техническими мероприятиями. К методическим приемам контроля относятся методики наблюдений, обработки и оценки результатов наблюдений для использования в целях управления. Организационные мероприятия обеспечивают непосредственную заинтересованность работников в качестве изготовляемой продукции.

Основной инструмент оперативного контроля за процессом приготовления и укладки гидротехнического бетона – контрольные карты для различных статистических параметров, вычисляемых по результатам наблюдений за процессом. Методика построения контрольных карт обуславливается видом контрольного процесса.

Выбор контролируемых параметров и процессов определяется их влиянием на качество гидротехнического бетона и однородность его свойств. Исследования показали [51, 52], что наибольшее влияние на однородность бетона Усть-Илимской ГЭС оказывают неточность сортирования заполнителей на границах фракций, неоднородность их гранулометрического состава (особенно песка), ошибки в дозировании цемента, колебания подвижности бетонной смеси. Изменчивость свойств цемента и добавок практически не регулируется на заводе, поэтому можно ограничиться учетом их влияния при назначении состава.

Проведенный анализ изменения во времени контролируемых факторов на основе построения автокорреляционных функций показал случайность их изменения во времени. В связи с этим технологические процессы рассматривались как случайные процессы одного из трех типов: стационарные в течение длительного периода (неделя, месяц), стационарные в течение короткого времени (смена, сутки) и нестационарные. Тип процесса определяли при помощи непараметрических критериев серий и тренда [18].

Анализ работы гравиесортировочного завода показал, что при установившейся технологии, такие характеристики, как изменение во времени модуля крупности песка, относительных количеств примесей на границах фракций являются стационарными (в течение не менее недели) случайными процессами с законами распределения, близкими

к нормальному. Стационарность процесса нарушается при изменении технологии, к примеру, размеров ячейки сит, или грубых нарушениях технологии (разрыв сит, завал грохота и т. д.). На гравиесортировочных заводах ведутся простые контрольные карты ежемесячных наблюдений за индивидуальными значениями модуля крупности песка, содержанием отмучиваемых частиц, относительным содержанием примесей смежных фракций. При наличии ряда наблюдений по контрольной карте можно легко судить о нарушениях технологии или об изменениях, которые привели к изменению одного из показателей. Для установления причин нарушений используется практический опыт службы эксплуатации и контроля.

Значительные изменения (от 10 до 25%) в содержании фракции крупнее 5 мм в песке, получаемом на двух гравиесортировочных заводах, привели к необходимости оперативного корректирования состава бетона. С этой целью по результатам испытаний проб песка из дозаторов на бетонных заводах ведется контрольная карта индивидуальных значений и скользящего среднего из десяти наблюдений (рис. 3).

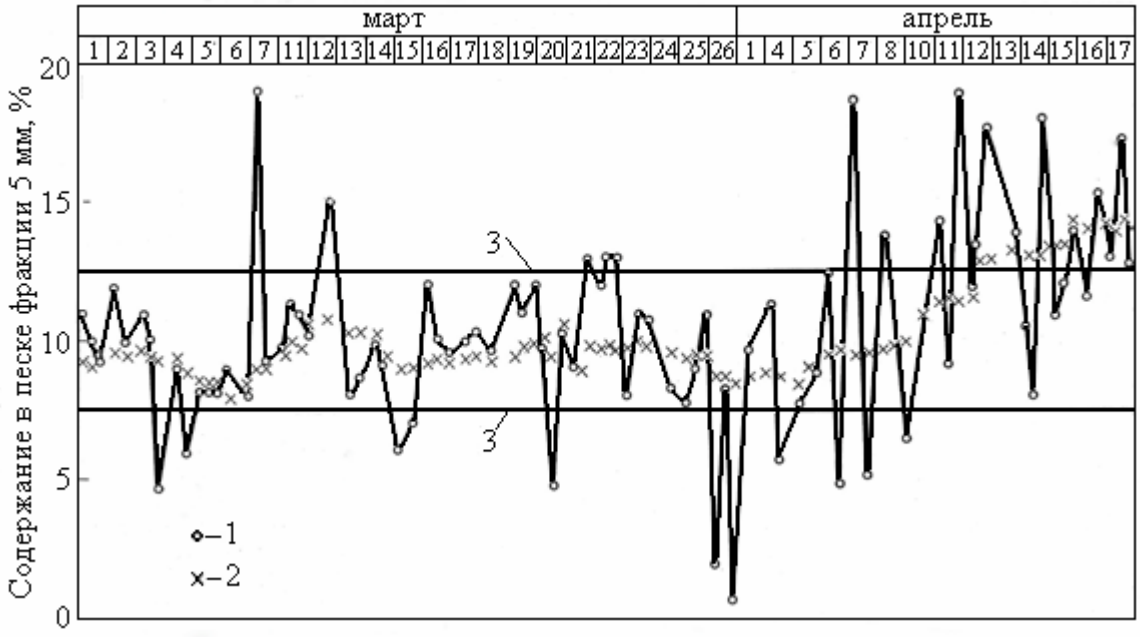


Рис. 3. Контрольная карта индивидуальных значений (1) и скользящего среднего (2) процентного содержания в песке фракции крупнее 5 мм; 3 — контрольные границы

Составы бетона корректируют через 5%-ные контрольные интервалы. Так, например, до 12 апреля бетонные заводы работали на составах, содержащих 10% гравия в песке, а с 12 апреля вследствие перехода скользящей средней через границу 12.5% составы были изменены с учетом содержания 15% гравия в песке.

Процесс дозирования компонентов бетонной смеси на заводах приготовления бетона следует рассматривать как случайный стационарный в течение короткого период времени (смена и иногда менее смены). Для оперативного контроля относительной ошибки дозирования были использованы толерантные контрольные карты [33–38] (рис. 4).

Применение таких карт позволяет обойтись небольшим объемом наблюдений за работой дозаторов в течение смены. Последовательный анализ Вальда [51–53] показал, что для характеристики процесса дозирования при условии его стационарности необходимо не менее девяти наблюдений. В целях оперативного контроля на заводах снимают по 10 наблюдений (взвешиваний) с каждого работающего дозатора каждую

смену. Показания снимают в случайные промежутки времени работы дозаторов, исключая процесс настройки. Границы отклонений от установленной составом нормы взвешивания взяты по СНиП III-В. 1-70: для цемента, воды и добавок – 2%, для заполнителей – 3%.

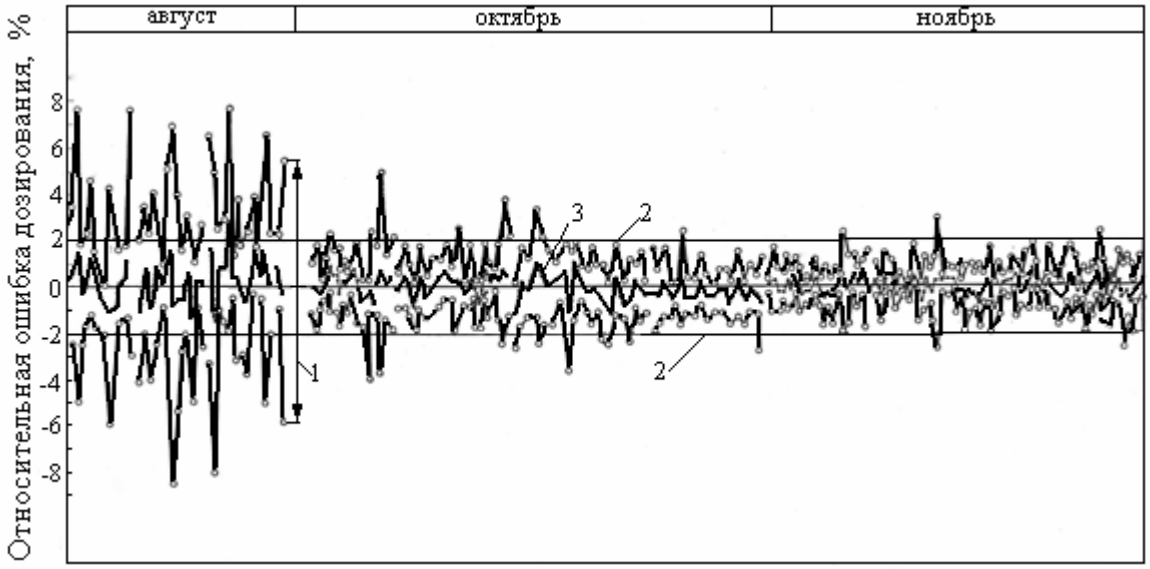


Рис. 4. Толерантная контрольная карта относительной ошибки дозирования цемента: 1 – толерантный интервал, 2 – нормативные контрольные границы, 3 – график средних значений

По результатам наблюдений за смену определяют среднее значение $\bar{a}$ и среднеквадратичное отклонение s относительной ошибки дозирования. Рассчитывается верхняя и нижняя границы толерантного интервала $K_{B.H.} = \bar{a} + \tau s$, в котором с заданной доверительной вероятностью (90%) лежит определенная доля генеральной совокупности (85%); τ — толерантный множитель. Доверительная вероятность определяет надежность контроля, т.е. зависит от того, как тщательно нужно организовать контроль. Доля генеральной совокупности должна определяться нормативными документами и нами условно перенесена с СНиП III-В. 1-70. Толерантный множитель $\tau = 1.96$ определяется объемом наблюдений $n = 10$, долей генеральной совокупности и доверительной вероятностью по табл. 4.2 [18]. Выход верхней и нижней границ толерантного интервала за нормативные границы сигнализирует о неблагополучном положении с точностью дозирования. При наличии контрольной карты видно, как работает дозатор во времени и является ли «плохая» смена случайным или систематическим явлением. Необходимо ясно представлять, что описанная контрольная карта не определяет причин плохой или хорошей работы дозаторов, а оперативно отражает действительное состояние процесса. Например, изменение конструкции затвора на дозаторе цемента привело к значительному повышению точности дозирования, что немедленно отразилось в контрольной карте (рис. 4).

Применение такого вида контрольных карт позволяет быстро обрабатывать результаты наблюдений и обеспечивает очень жесткий контроль. Периодические выборки по 50 и более взвешиваний подтвердили, что при удержании границ в нормативных пределах, точность дозирования, заданная в исходных требованиях, строго обеспечивается.

Использование контрольных карт распространяется на выходные параметры бетонной смеси: температура, подвижность, прочность. Поскольку изменение температуры во времени – нестационарный случайный процесс, он контролируется при помощи карты индивидуальных значений (рис. 5). Управление температурой бетонной смеси велось для зимнего периода с ноября по апрель. Отдельные значения температуры сравниваются с контрольными границами, определяемыми по заданной для местных условий зависимости допускаемых температур бетонной смеси от температуры наружного воздуха. Выход результатов замера температуры за границы в ряде случаев приводит к остановке секций бетонных заводов для исправления положения.

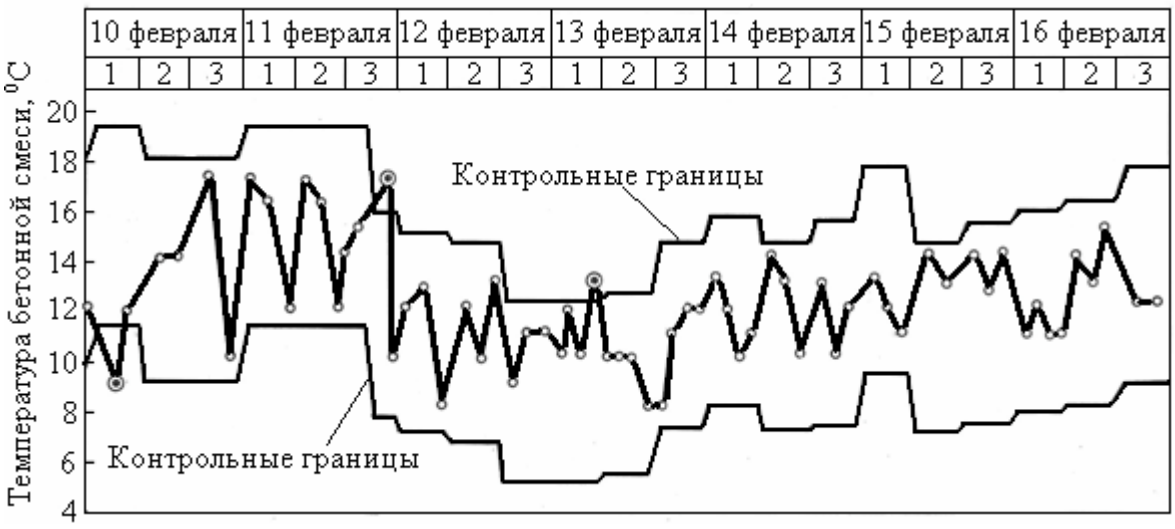


Рис. 5. Контрольная карта индивидуальных значений температуры бетонной смеси

Выполнение нормативных требований к прочности бетона контролируется при помощи величины скользящей минимальной фактической прочности $R^{ф}_{мин}$ в серии по соотношению

$$R^{ф}_{мин} = \breve{R} - \tau_R S_R \geq R_{норм},$$

где

$\breve{R}$ — скользящая средняя прочность из девяти серий образцов (серия образцов – группа контрольных образцов-кубов, изготовленных из одной пробы бетонной смеси, твердевших в одинаковых условиях и испытанных в одном возрасте);

S_R — скользящее среднеквадратическое отклонение прочности из девяти серий образцов;

τ_R — толерантный множитель;

$R_{норм}$ — нормируемая прочность на момент испытания.

Доля генеральной совокупности $\beta = 0.85$, лежащая за нормативным значением прочности, условно перенесена из ГОСТ 18105-72. Это определило при заданной доверительной вероятности $p = 0.90$ толерантный множитель $\tau_R = 1.5$ [18].

В целях оперативного определения прочности после изготовления (нормативный возраст 180 суток) приходится пользоваться результатами испытаний в ранние сроки, поэтому $R_{норм}$ на момент испытаний определяли по полученным регрессионным

зависимостям между R_{28} и R_{180}, R_7 и R_{180} по результатам пассивного эксперимента для Усть-Илимских бетонов.

Контрольная карта $R^{ф}_{мин}$ (рис. 6) отражает тенденцию изменения прочности во времени и уровень минимальной прочности относительно нормируемого. Карта используется для анализа влияния изменения состава бетона, качества исходных материалов, сезона работы и т.п. Так, в конце апреля был изменен состав бетона, после чего не было отмечено резкого повышения или снижения прочности, и были выполнены нормативные требования, а, следовательно, изменение состава посчиталось правильным (рис. 6).

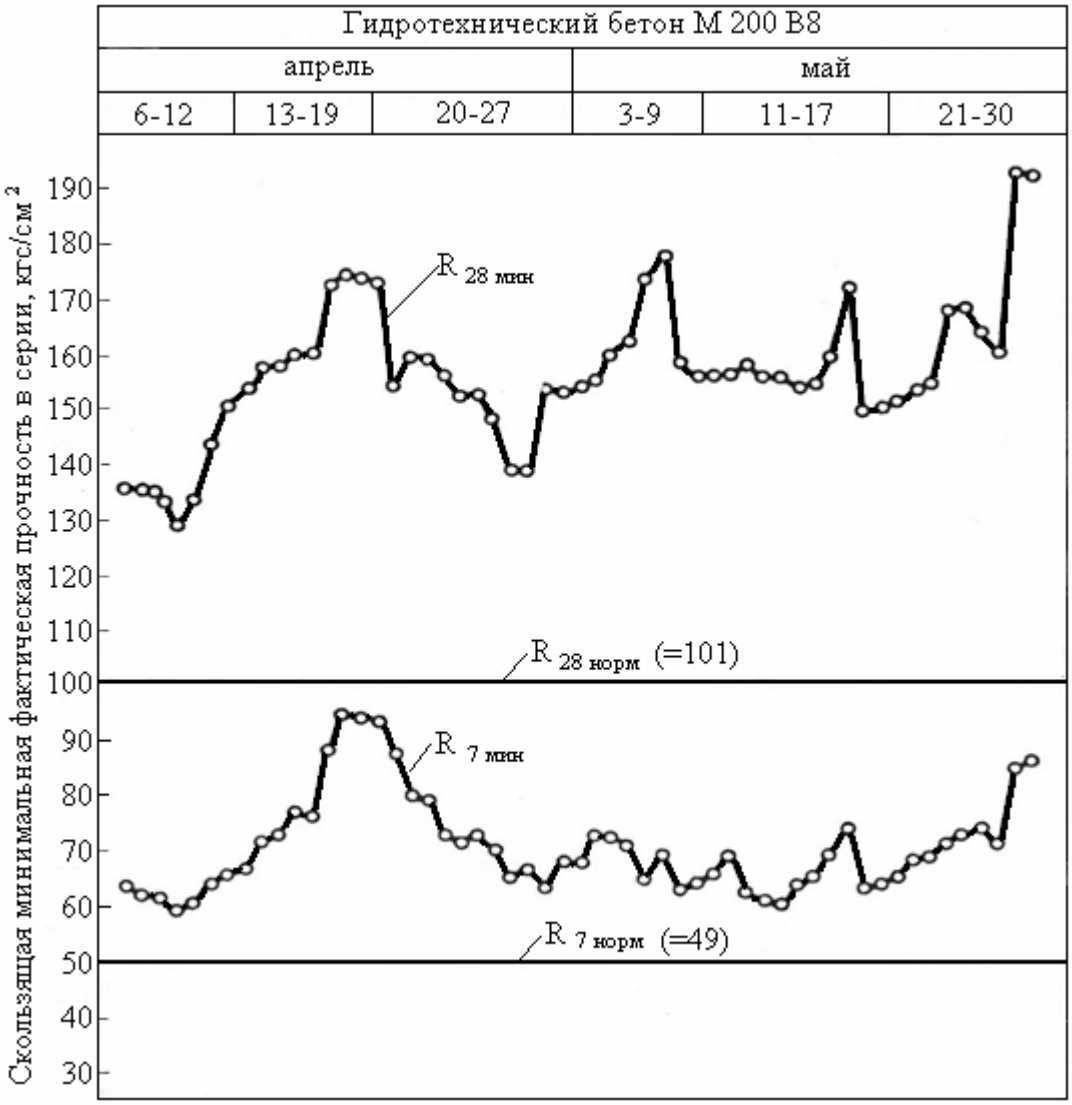


Рис. 6. Контрольная карта скользящей минимальной фактической прочности в серии для бетона М200 В8

При разных методиках определения однородности и оценки прочности бетона М200 В8 получены результаты, подтверждающие выполнение всех нормативных требований.

Система статистического контроля и управления качества, внедренная на строительстве Усть-Илимской ГЭС, привела к существенному повышению оператив-

ности получения информации о нарушениях технологических процессов, значительному упорядочиванию и унификации документации, улучшению наглядности. Система позволяет вести строгий и чёткий контроль за разнообразными технологическими процессами при значительном меньшем объёме требуемых наблюдений. Это привело к уменьшению расхода цемента в бетонах. Например, в бетоне основной марки 200 В8 для строительства плотины расход цемента на 10 кг меньше, чем на строительстве Братской ГЭС.

Улучшение гранулометрического состава мелких заполнителей

Изготовление бетонной смеси, предназначенной для выполнения ответственных конструкций, предшествует специальная подготовка нерудных заполнителей. Важное значение при этом имеет улучшение гранулометрического состава песка и связанной с ней однородности свойств бетона.

Представим гранулометрический состав исходного песка (отсеянного из песчано-гравийной смеси) в частных остатках на i ситах как $\alpha_i, i = 1,2,\ldots,n$. Из-за естественной неоднородности состав песка меняется, при этом величины частных остатков на отдельных ситах – случайные величины, распределенные по нормальному закону. Они могут быть охарактеризованы математическими ожиданиями $\mu(\alpha_i)$ и дисперсиями $\sigma^2(\alpha_i)$.

Разделение песка на отдельные фракции (в нашем случае крупную и мелкую) происходит по определенной границе, на которую настроена работа гидравлического классификатора. Содержание в исходном песке частиц крупнее β_1 и мельче β_2 границы раздела изменяются по усеченному нормальному закону распределения. При этом всегда $\beta_1 + \beta_2 = 1$. Эти случайные величины могут быть также охарактеризованы математическими ожиданиями $\mu(\beta_1)$, $\mu(\beta_2)$ и дисперсиями $\sigma^2(\beta_1)$, $\sigma^2(\beta_2)$. Тогда $\mu(\beta_2) = 1 - \mu(\beta_1)$ и с высокой точностью $\sigma^2(\beta_1) = \sigma^2(\beta_2) = \sigma^2(\beta)$.

Величина дисперсии $\sigma^2(\beta)$ определяется естественным колебанием содержания частиц мельче или крупнее границы раздела в исходном песке и неточностью классификации. Теоретически при абсолютной точности классификации величина $\sigma^2(\beta)$ зависит только от неоднородности гранулометрического состава исходного продукта.

Гранулометрический состав отдельных фракций характеризуется математическими ожиданиями частных остатков $\mu_1(\alpha_i)$, $\mu_2(\alpha_i)$ и дисперсиями $\sigma_1^2(\alpha_i)$, $\sigma_2^2(\alpha_i)$. Вследствие независимости случайных величин α и β математические ожидания и дисперсии частных остатков исходного песка

$$\mu(\alpha_i) = \mu_2(\alpha_i) + \mu(\beta_1)(\mu_1(\alpha_i) - \mu_2(\alpha_i)), \tag{1}$$

$$\sigma^2(\alpha_i) = \sigma^2(\beta)(\sigma_1^2(\alpha_i) + \sigma_2^2(\alpha_i) + \mu_1^2(\alpha_i) + \mu_2^2(\alpha_i)) + \mu_1^2(\alpha_i)\sigma_1^2(\alpha_i) + \mu_2^2(\alpha_i)\sigma_2^2(a_i), \quad i = 1,2,\ldots,n \tag{2}$$

Аналогично решается задача смешивания отдельных фракций через дозирующие устройства с заданным содержанием – случайные величины $\beta_1^{см}$, $\beta_2^{см}$, $\beta_1^{см} + \beta_2^{см} = 1$. Дозирование – процесс случайный, стационарный, центрированный и нормально распределенный с дисперсией $\sigma_{доз}^2$ и независимый от случайных величин α и β. По опыту работы дозаторов песка в Усть-Илимском бетонном хозяйстве, дисперсия $\sigma_{доз}^2$ не зависит от нормы взвешивания и может быть принята постоянной, а математические

ожидания равны $\mu\left(\beta_1^{см}\right)$ и $\mu\left(\beta_2^{см}\right)=1-\mu\left(\beta_1^{см}\right)$. Тогда математические ожидания и дисперсии частных остатков исходного песка после смешивания

$$\mu\left(\alpha_i^{см}\right)=\mu_2(\alpha_i)+\mu\left(\beta_1^{см}\right)\left(\mu_1(\alpha_i)-\mu_2(\alpha_i)\right), \tag{3}$$

$$\sigma^2\left(\alpha_i^{см}\right)=\sigma_{доз}^2\left(\sigma_1^2(\alpha_i)+\sigma_2^2(\alpha_i)+\mu_1^2(\alpha_i)+\mu_2^2(\alpha_i)\right)+\mu_1^2(\alpha_i)\sigma_1^2(\alpha_i)+\mu_2^2(\alpha_i)\sigma_2^2(\alpha_i), \quad i=1,2,...,n \tag{4}$$

Сравнивая выражения (1) и (3), видим, что, если $\mu(\beta_1)=\mu\left(\beta_1^{см}\right)$, то $\mu(\alpha_i)=\mu\left(\alpha_i^{см}\right)$, то есть при дозировании фракций в количестве, равном их среднему содержанию в исходном песке, средний гранулометрический состав песка, полученного после смешивания, сохранится.

В тоже время однородность гранулометрического состава, оцениваемая дисперсией на каждом i-м сите, изменится. Как видно из сравнения выражений (2) и (4), дисперсия уменьшится вследствие разницы между дисперсиями $\sigma^2(\beta)$ и $\sigma_{доз}^2$. При $\sigma_{доз}^2<\sigma^2(\beta)$ однородность повысится.

Рассчитывался эффект улучшения однородности песка за счет его разделения на две фракции с последующим смешиванием на примере песка, используемого на строительстве Усть-Илимской ГЭС [50]. При этом приняты следующие допущения:

- исходный продукт – промытый на спиральных классификаторах песок летней сортировки;
- абсолютная точность классификации – на границе 0.63 мм (фракции крупнее и мельче 0.63 мм разделяются без захвата);
- после разделения гранулометрический составов отдельных фракций не изменяется.

Исходные данные для расчета в виде выборочных оценок математических ожиданий и дисперсий по результатам лабораторных анализов и наблюдений за точностью дозирования составляют: $\mu(\beta_1)=\mu\left(\beta_1^{см}\right)=0.43$; $\sigma(\beta)=0.07$; $\sigma_{доз}^2=0.02$. Расчет проводится для частных остатков на ситах 0.14; 0.315 — мелкая фракция; 0.63; 1.25; 5.00 — крупная фракция, которые обозначаются 1,2,…,5. Для исходного песка выборочные оценки математических ожиданий и дисперсий: $\mu(\alpha_1)=25.5\%$; $\mu(\alpha_2)=23.7\%$; $\mu(\alpha_3)=8.5\%$; $\mu(\alpha_4)=26.7\%$; $\mu(\alpha_5)=15.6\%$; $\sigma(\alpha_1)=6.3\%$; $\sigma(\alpha_2)=3.5$ %; $\sigma(\alpha_3)=1.8\%$; $\sigma(\alpha_4)=2.3\%$; $\sigma(\alpha_5)=2.5\%$.

Для крупной фракции, отношение дисперсий $K_i^{кр}=\sigma_{кр}^2(\alpha_i)/\sigma_{кр}^2\left(\alpha_i^{см}\right)$, $i=1,2,...,n$, определяет эффект повышения однородности, где $\sigma_{кр}^2(\alpha_i)$ и $\sigma_{кр}^2\left(\alpha_i^{см}\right)$определяется формулами (2), (4) при $\mu_2(\alpha_i)=0$, $\sigma_2^2(\alpha_i)=0$, так как нет захвата в крупную фракцию из мелкой. Для мелкой фракции расчёты аналогичны.

Величина $K_i^{кр}$ (в зависимости от размера сит составляет): 0.14 мм – 1.5; 0.315 мм – 2.7; 0.63 мм – 1.7; 1.25 мм – 2.2; 5 мм – 1.2. Таким образом, однородность частных остатков (узких фракций) песка улучшается неодинаково, так как зависит от соотношения математических ожиданий $\mu(\alpha_i)$ и дисперсий $\sigma^2(\alpha_i)$.

В действительности, точность классификации песка далека от абсолютной, и это неизбежно скажется на величинах $\sigma^2(\beta)$, $\sigma_1^2(\alpha_i)$ и $\sigma_2^2(\alpha_i)$. В таком случае эффект повышения однородности будет несколько снижен.

Величина дисперсии $\sigma_{доз}=0.02$ взята нами для порционных дозаторов бетонного завода. При этом следует отметить высокую точность дозирования, вследствие этого,

величиной $\sigma^2_{доз}$ можно практически пренебречь. При низкой точности дозирования ($\sigma_{доз} = 0.03$ и более) влияние этого фактора будет существенно и может привести к минимуму все усилия по улучшению однородности.

Таким образом, чтобы улучшить однородность гранулометрического состава песка, необходимо выполнить главное условие, а именно $\sigma^2_{доз} < \sigma^2(\beta)$, кроме того, следует обеспечить наилучшее разделение песка на границе раздела.

Рассмотрим другой способ повышения однородности песка – смешивание двух или более независимых потоков в равных соотношениях. Практически два или более независимых потока исходного промытого песка дозируется в равных соотношения на одну транспортёрную ленту. Для этой цели может быть использован узел шихтовки (рис. 7). Вместо фракций, полученных разделением на гидравлическом классификаторе, в штабели укладывают песок одной фракции (0–5 мм) из отдельных технологических потоков. В узел непрерывного дозирования песок подают независимыми потоками, что обеспечивает случайность гранулометрического состава песка перед его смешиванием. Все расчёты могут быть выполнены по аналогам формул (3) и (4) для любого количества независимых потоков. В данном случае, также большое значение имеет точность дозирования, характеризуемая дисперсией ошибки $\sigma^2_{доз}$.

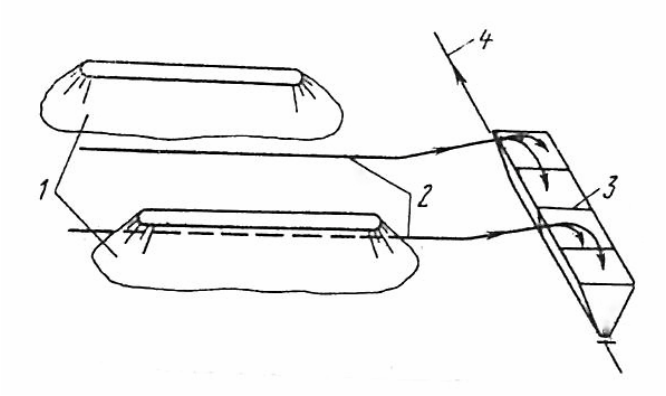


Рис. 7. Узел шихтовки: 1 – штабеля песка; 2 – независимые потоки; 3 – узел непрерывного дозирования; 4 – поток смешанного песка

Эффект улучшения однородности гранулометрического состава песка K_i в случае строительства Усть-Илимской ГЭС подсчитан для двух и трех потоков в зависимости от размера сит: 0.14 мм – 1.7; 2.3; 0.315 мм – 1.6; 2.0; 0.63 мм – 2.0; 2.8; 125 мм – 2.0; 2.6; 5 мм – 1.7; 2.3.

Выводы

Сравнивая эффект улучшения однородности при разделении на фракции и смешивания независимых потоков, можно сделать вывод о том, что повышение однородности смешиванием потоков равноценно классификации песка. Главным условием, при котором можно обойтись без классификации, применяя более простой способ смешивания, является относительно небольшая величина $\sigma(\beta)$ в исходном песке (колебания в содержании фракций крупнее и мельче границы раздела), как это показано на примере усть-илимского песка.

Итак, разработанная методика позволяет оценить эффект улучшения однородности мелких материалов при их разделении на фракции и последующем смешивании с учетом воздействия основных технологических факторов. Следует также отметить, что смешивание независимых потоков песка приносит значительную экономию материальных средств в сравнении с методом гидравлической классификации песка на фракции.

Список литературы

1. Вероятность и математическая статистика [Текст] : энцикл. / Российский фонд фундаментальных исследований ; Гл. ред. Ю.В. Прохоров. — М. : Большая Рос. энцикл., 1999. — 910 с.
2. Крамер, Г. Математические методы статистики [Текст] = Mathematical Methods of Statistics : научное издание / Г. Крамер ; ред. А.Н. Колмогоров ; пер.: А.С. Монин, А.А. Петров. — М. : Гос. изд-во иностр. лит., 1948. — 632 с.
3. Крамер, Г. Математические методы статистики = Mathematical methods of statistics / Г. Крамер ; пер. с англ. А.С. Монина, А.А. Петрова под ред. А.Н. Колмогорова. — Изд. 2-е, стер. — М. : Мир, 1975. — 648 с.
4. Налимов, В.В. Применение математической статистики при анализе вещества / В.В. Налимов. — М.: Физматгиз, 1960. — 431 с.
5. Романовский, В.И. Математическая статистика [Текст] / В.И. Романовский ; Акад. наук УзССР. Ин-т математики им. В.И. Романовского. — Ташкент : Изд-во Акад. наук УзССР, 1961. — . —
   Кн. 1 : Основы теории вероятностей и математической статистики. — 1961. — 637 с.
6. Романовский, В.И. Математическая статистика [Текст] / В.И. Романовский ; Акад. наук УзССР. Ин-т математики им. В.И. Романовского. — Ташкент : Изд-во Акад. наук УзССР, 1963. — . —
   Кн. 2 : Оперативные методы математической статистики. — 1963. — 794 с.
7. Гренандер, У. Случайные процессы и статистические выводы [Текст] / У. Гренандер ; пер. с англ. и доп. А.М. Яглома. — М. : Изд-во иностр. лит., 1961. — 167 с.
8. Уилкс, С. Математическая статистика [Текст] : научно-популярная литература / С. Уилкс ; пер.: А.М. Каган, Л.А. Халфин, О.В. Шалаевский ; ред. Ю.В. Линник. — М. : Наука, 1967. — 632 с.
9. Дженкинс, Г. Спектральный анализ и его приложения = Spectral analysis and its applications / Г. Дженкинс, Д. Ватт. — М. : Мир, 1971-1972. — . —
   Вып. 1 / пер. с англ. В.Ф. Писаренко ; с предисл. А.М. Яглома. — 316 с.
   Вып. 2 / пер. с англ. В.Ф. Писаренко ; с предисл. А.М. Яглома. — 287 с.
10. Кендалл, М. Теория распределений [Текст] = Distribution Theory : научное издание / М. Кендалл, А. Стьюарт ; пер.: В.В. Сазонов, А.Н. Ширяев ; ред. А.Н. Колмогоров. — М. : Наука, 1966. — 587 с.
11. Кендалл, М. Статистические выводы и связи [Текст] = The advanced theory of statistics : монография / М. Кендалл, А. Стьюарт ; под ред. А.Н. Колмогоров. — М. : Наука. Главная редакция физико-математической литературы [Физматлит], 1973. — 899 с.
12. Кендалл, М. Многомерный статистический анализ и временные ряды [Текст] : пер. с англ. / М. Кендалл, А. Стьюарт ; ред.: А.Н. Колмогоров, Ю.В. Прохоров. — М. : Наука, 1976. — 736 с.
13. Бендат Дж. Измерение и анализ случайных процессов = Random data: analysis and measurement procedures / Дж. Бендат, А. Пирсол ; пер. с англ. Г.В. Матушевского, В.Е. Привальского ; с предисл. Г.Я. Мирского. — М. : Мир, 1974. — 463 с.
14. Андерсон, Т. Статистический анализ временных рядов [Текст] : монография / Т. Андерсон; Пер. с англ. И.Г. Журбенко, В.П. Носко; Под ред. Ю.К. Беляева. — М. : Мир, 1976. — 755 с.
15. Беляев, Ю.К. Вероятностные методы выборочного контроля [Текст] / Ю.К. Беляев. — М. : Наука, 1975. — 407 с.
16. Тутубалин, В.Н. Границы применимости. Вероятностно-статистические методы и их возможности [Текст] / В.Н. Тутубалин. — М. : Знание, 1977. — 64 с.
17. Гнеденко, Б.В. Математика и контроль качества продукции [Текст] : научное издание / Б.В. Гнеденко. — 2-е изд., испр. — М. : Изд-во ЛКИ, 2007. — 63 с.
18. Большов, Л.Н. Таблицы математической статистики [Текст] / Л.Н. Большев, Н.В. Смирнов. — 3-е изд. — М. : Наука, 1983. — 416 с.

19. Орлов, А.И. Что дает прикладная статистика народному хозяйству? / А.И. Орлов // Вестник статистики. — 1986. — № 8. — С. 52–56.
20. Журбенко, И.Г. Анализ стационарных и однородных случайных систем [Текст] : учеб. пособие для студ. вузов, обуч. по спец.: Математика / И.Г. Журбенко. — М. : МГУ, 1987. — 240 с.
21. Колмогоров, А.Н. Вероятностно-статистические методы обнаружения спонтанно возникающих эффектов / А.Н. Колмогоров, Ю.В. Прохоров, А.Н. Ширяев // Труды Математического института им. В.А. Стеклова [Текст].Теория вероятностей, теория функций, механика : сб. обзорных ст.: к 50-летию Института, вып. 5 / АН СССР ; ред. Ю.В. Прохоров. — М. : Наука, 1988. — С. 4–23.
22. Орлов, А.И. О перестройке статистической науки и её применении / А.И. Орлов // Вестник статистики. — 1990. — № 1. — С. 65–71.
23. Орлов, А.И. Сертификация и статистические методы / А.И. Орлов // Заводская лаборатория. Диагностика материалов. — 1997. — Том 63, № 3. — С. 55–62.
24. Орлов, А.И. Термины и определения в области вероятностно-статистических методов / А.И. Орлов // Заводская лаборатория. Диагностика материалов. — 1999. — Том 65, № 7. — С. 46–54.
25. Орлов, А.И. Прикладная статистика XXI в. / А.И. Орлов // Экономика XXI века. — 2000. — № 9. — С. 3–27.
26. Колмогоров, А.В. Избранные труды : в 6 т. / А.Н. Колмогоров ; Рос. акад. наук, Отд-ние мат. наук, Мат. ин-т им. В.А. Стеклова. — М. : Наука, 2005. — . —
Т. 2 : Теория вероятностей и математическая статистика. — 2005. — 581 с.
27. Кудлаев, Э.М. Вероятностно-статистические методы исследования в работах А.Н. Колмогоров / Э.М. Кудлаев, А.И. Орлов // Заводская лаборатория. Диагностика материалов. — 2003. — Том 69, № 5. — С. 55–61.
28. Орлов, А.И. Математические методы исследования в работах Бориса Владимировича Гнеденко / А.И. Орлов // Заводская лаборатория. Диагностика материалов. — 2007. — Том 73, № 7. — С. 66–72.
29. Грановский, Ю.В. К 100-летию со дня рождения В.В. Налимова: поиск нового на перекрестке наук / Ю.В. Грановский, Е.В. Маркова // Заводская лаборатория. Диагностика материалов. — 2010. — Том 76, № 7. — С. 60–68.
30. Горский, В.Г. Прикладная математическая статистика – наш профиль / В.Г. Горский // Заводская лаборатория. Диагностика материалов. — 2007. — Том 73, № 1. — С. 96–100.
31. Шор, Я.Б. Статистические методы анализа и контроля качества и надежности [Текст] / Я.Б. Шор. — М. : Сов. радио, 1962. — 552 с.
32. Гнеденко, Б.В. Математические методы в теории надежности. Основные характеристики надежности и их статистический анализ [Текст] : монография / Б.В. Гнеденко, Ю.К. Беляев, А.Д. Соловьев. — М. : Наука, 1965. — 524 с.
33. Даниленко, Е.Л. Оперативное статистическое управление качеством продукции / Е.Л. Даниленко // Материалы Всесоюзного совещания по проблемам управления. — Минск, 1977.
34. Даниленко, Е.Л. Математико-статистические и вероятностные методы оперативного контроля случайных процессов / Е.Л. Даниленко. — 29 с. — Деп. в ВИНИТИ 03.04.81, № 1482-81.
35. Даниленко, Е.Л. Математико-статистические и вероятностные модели оперативного контроля случайных процессов / Е.Л. Даниленко // V Всесоюзное совещание по статистическим методам в процессах управления. — М. : ИПУ АН СССР, 1981. — С. 45–54.
36. Даниленко, Е.Л. Математико-статистические методы оперативного контроля случайных процессов / Е.Л. Даниленко // Исследование операций и АСУ. — Киев: Вища школа, 1982. — Вып. 19. — С. 31–39.
37. Даниленко, Е.Л. Статистический контроль функционирования некоторой динамической системы / Е.Л. Даниленко // Динамика систем: межвуз. научн. сб. — Омск: ОмПИ, 1984.
38. Даниленко, Е.Л. Стохастические модели контроля сложных технических систем: монография / Е.Л. Даниленко. — 279 с. — Деп. в ВИНИТИ 13.06.84, № 3891-84.
39. Лумельский, Я.П. Статистические оценки результатов контроля качества [Текст] / Я.П. Лумельский. — М. : Изд-во стандартов, 1979. — 200 с.
40. Мердок, Дж. Контрольные карты [Текст] : научное издание / Дж. Мердок ; пер. с англ. С.А. Фатеева. — М. : Финансы и статистика, 1986. — 151 с.
41. Кривцов, В.С. Современные статистические методы в стандартизации и управлении качеством продукции / В.С. Кривцов, А.И. Орлов, В.Н. Фомин // Стандарты и качество. – 1988. – № 3. – С. 32–36.
42. Статистические методы повышения качества [Текст] : монография: Пер. с англ. / ред. Х. Кумэ ; пер.: Ю.П. Адлер, Л.А. Конарева. — М. : Финансы и статистика, 1990. — 301 с.

43. Орлов, А.И. Статистический контроль качества продукции / А.И. Орлов // Российское предпринимательство. — 2001. — № 2(14). — С. 17–24.
44. Смирнова, О.С. Программное обеспечение для статистического анализа / О.С. Смирнова // Заводская лаборатория. Диагностика материалов. — 2008. — Том 74, № 5. — С. 68–75.
45. Даниленко, Е.Л. Некоторые методологические вопросы статистического контроля и управления качеством процессов / Е.Л. Даниленко // Проблемы статистического измерения, моделирования, прогнозирования научно-технического прогресса. — М.: МЭСИ, 1974.
46. Даниленко, Е.Л. Об использовании обобщенного приведенного показателя качества / Е.Л. Даниленко // Заводская лаборатория. — 1975. — № 1.
47. Даниленко, Е.Л. Метод балльных оценок для контроля качества технологических процессов / Е.Л. Даниленко, П.Я. Старожицкий // Стандарты и качество. — 1975. — № 10. — С. 40–41, 62.
48. Даниленко, Е.Л. Система балльных оценок качества бетонных работ на строительстве Усть-Илимской ГЭС / Е.Л. Даниленко, М.А. Садович // Гидротехническое строительство. — 1976. — № 7. — С. 7–9.
49. Даниленко, Е.Л. Исследование возможности приготовления бетонов на несортированной гравийно-песчаной смеси при помощи математико-статистических методов / Е.Л. Даниленко [и др.] // Применение методов моделирования с целью совершенствования технологии производства строительных материалов. — Тольятти, 1974. — С. 120–126.
50. Даниленко, Е.Л. Улучшение гранулометрического состава мелких заполнителей / Е.Л. Даниленко, М.А. Садович // Строительные материалы. — 1975. — № 9. — С. 27–28.
51. Даниленко, Е.Л. Система статистического контроля и управления качеством бетона на строительстве Усть-Илимской ГЭС / Е.Л. Даниленко, М.А. Садович, П.Я. Старожицкий // Энергетическое строительство. — 1974. — № 2. — С. 43–47.
52. Даниленко, Е.Л. Статистический контроль и управление качеством бетона / Е.Л. Даниленко, М.А. Садович // Бетон и железобетон. — М.: Стройиздат, 1975. — № 1. — С. 10–11.
53. Вальд, А. Последовательный анализ / А. Вальд ; пер. с англ. П.А. Бакута [и др.] ; под ред. Б.А. Севостьянова. — М. : Физматгиз, 1960. — 327 с.

ЕФЕКТИВНЕ ЗАСТОСУВАННЯ МАТЕМАТИКО–СТАТИСТИЧНІХ МЕТОДІВ

Е.Л. Даніленко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: sankirillo@yahoo.com

Пропонуються приклади ефективного використання простих математико-статистичних методів в промисловому і будівельному виробництві.

Ключові слова: статистичні оцінки, бальні оцінки, статистичний контроль якості, контрольні карти, однорідність гранулометричного складу, якість бетону

EFFECTIVE USE OF MATHEMATICAL STATISTICS

Eugene L. Danilenko

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: sankirillo@yahoo.com

The examples of the effective use of simple mathematical statistics methods are offered in an industrial and build production.

Keywords: statistical estimations, numerical scores, statistical control of quality, control cards, homogeneity of particle-size, concrete quality

УДК 004.056.5: 518: 512.624.3

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 2, pp. 146-155

SIGN-НЕЧУВСТВИТЕЛЬНОСТЬ СИНГУЛЯРНЫХ ВЕКТОРОВ МАТРИЦЫ ИЗОБРАЖЕНИЯ КАК ОСНОВА СТЕГАНОАЛГОРИТМА, УСТОЙЧИВОГО К СЖАТИЮ

М.А. Мельник

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: ritochek@yandex.ru

В работе на основе sign-нечувствительности, обеспечивающей нечувствительность сингулярных векторов стандартных блоков матрицы цифрового изображения, отвечающих максимальным сингулярным числам, к произвольным возмущающим воздействиям, разработан полиномиальный степени 2 стеганографический алгоритм, устойчивый к сжатию со значительными коэффициентами. Приведены результаты вычислительного эксперимента, подтверждающие эффективность предложенного алгоритма.

Ключевые слова: сингулярный вектор, сингулярное число, sign-чувствительность, возмущающее воздействие, сжатие, матрица

Введение

Стеганография сегодня переживает этап своего бурного развития. Однако многообразие современных стеганографических методов и алгоритмов (СА) не изменяет требований, предъявляемых к ним, среди которых наиболее важными являются: надежность восприятия формируемого стеганосообщения (СС), являющегося результатом погружения дополнительной информации (ДИ) в непривлекающий внимание контейнер, или основное сообщение (ОС), в качестве которого в настоящей работе рассматривается цифровое изображение (ЦИ); устойчивость к преднамеренным (непреднамеренным) атакам [1, 2], среди которых одно из центральных мест занимает атака сжатием. Согласно [2], под устойчивостью (неустойчивостью) СА будем понимать нечувствительность (чувствительность) к возмущающим воздействиям сформированного им СС.

Проблема создания СА, устойчивых к атаке сжатием, которая является чрезвычайно распространенной благодаря популярности использования форматов с потерями для хранения и передачи цифровых сигналов, является актуальной, но не решенной на сегодняшний день. Чаще всего существующие СА такого плана осуществляют погружение ДИ в частотной области контейнера и, при условии обеспечения надежности восприятия СС, выдерживают лишь незначительное сжатие [3–6].

Согласно общему подходу к анализу состояния и технологии функционирования информационных систем [2, 7], процесс СП можно представить как возмущение ΔF матрицы F контейнера: $\overline{F} = F + \Delta F$, где $\overline{F}$ — матрица СС, а потому СП формально представляется как совокупность возмущений сингулярных чисел (СНЧ) и сингулярных векторов (СНВ) соответствующей матрицы (матриц) ОС [7]. В силу этого о свойствах получаемого СС, в частности, о его чувствительности к атаке сжатием, можно судить по характерным особенностям СНВ и/или СНЧ, свойствам их возмущений, произошедших в ходе погружения ДИ.

В [8] были получены достаточные условия для формального представления СП как совокупности возмущений СНВ матриц, отвечающих контейнеру, обеспечивающие нечувствительность (малую чувствительность) формируемого СС к сжатию: формальным представлением процесса СП должна быть совокупность возмущений левых и/или правых СНВ блоков матрицы контейнера, полученных после ее стандартного разбиения, отвечающих (отвечающего) максимальным СНЧ блоков; при организации СП погружение ДИ должно происходить так, чтобы возмущение обсуждаемого (обсуждаемых) СНВ блоков оставляло его (их) близким к *n*-оптимальному вектору пространства R^8. Последнее требование обусловлено следующим. Независимо от возмущающего воздействия, которое претерпевает ЦИ, матрицы его блоков остаются неразложимыми неотрицательными [9], а обсуждаемые СНВ после любого возмущающего воздействия имеют все положительные координаты, поэтому эти векторы является не только нечувствительными, но и sign-нечувствительными к любому возмущающему воздействию [10], причем это свойство им присуще как до, та и после возмущающего воздействия, которое оставляет матрицу блока неразложимой неотрицательной, что возможно лишь в том случае, когда обсуждаемые СНВ близки к *n*-оптимальному [8]. Использование sign-нечувствительности СНВ блоков матрицы ОС дает принципиальную возможность для разработки СА, устойчивых к сжатию с большими (произвольными) коэффициентами.

Цель исследования и постановка задачи

Везде ниже атака сжатием на СС будет моделироваться путем его пересохранения в среде *Adobe* Photoshop в самый распространенный на сегодня формат с потерями для хранения ЦИ – формат JPEG с различными коэффициентами качества Q. Будем говорить, что сжатие происходит со значительным коэффициентом в случае, когда $Q \le 7$ [11].

Целью настоящей работы является повышение эффективности организации скрытого канала связи путем разработки нового стеганографического алгоритма, устойчивого к сжатию, в том числе со значительными коэффициентами, на основе полученных в [8] формальных достаточных условий нечувствительности (малой чувствительности) СС к сжатию в случае формального представления СП в виде совокупности возмущений СНВ блоков матрицы ОС.

Для достижения поставленной цели необходимо решить следующие *задачи*:

1) Расширить по сравнению с [8] набор качественных и количественных характеристик СНВ, отвечающих максимальным СНЧ блоков матрицы ЦИ, их возмущений в процессе сжатия с различными коэффициентами;

2) Выявить зависимость количественных оценок sign-нечувствительности СНВ, отвечающих максимальным СНЧ блоков ЦИ, от коэффициента сжатия;

3) Выявить зависимость количественных оценок sign-нечувствительности СНВ, отвечающих максимальным СНЧ блоков ЦИ, от формата хранения ЦИ;

4) На основе полученных количественных оценок sign-нечувствительности СНВ разработать стеганоалгоритм, устойчивый к сжатию со значительными коэффициентами.

Основная часть

Пусть матрица изображения F имеет размеры $m \times n$. Предварительным шагом при организации сжатия является стандартное разбиение F на 8×8-блоки. Обозначим B — матрицу отдельного блока. Для каждого блока возможно построение нормального

сингулярного разложения [7]: $B = U\Sigma V^T$, где U, V — ортогональные матрицы размера 8×8, столбцы $u_1,...,u_8$ матрицы U, называемые левыми СНВ, лексикографически положительны [7] (столбцы $v_1,...,v_8$ матрицы V — правые СНВ матрицы B); $\Sigma = diag(\sigma_1,...,\sigma_8)$, $\sigma_1 \ge ... \ge \sigma_8 \ge 0$ — СНЧ. В [7] показано, что невырожденная матрица имеет единственное нормальное сингулярное разложение, если ее СНЧ попарно различны. Далее считаем, что матрицы блоков ЦИ удовлетворяют условию единственности нормального сингулярного разложения.

Близость СНВ блоков матрицы ЦИ (u_1, v_1), отвечающие наибольшим СНЧ (σ_1), к n-оптимальному вектору пространства R^8 [8] приводит к тому, что углы между векторами u_1 и n-оптимальным, v_1 и n-оптимальным, а потому и между u_1 и v_1 для подавляющего большинства блоков изображения имеют малые значения. Sign-нечувствительность u_1 и v_1 влечет за собой нечувствительность этих СНВ к любым возмущающим воздействиям: их отклонение от первоначального положения, в частности, при сжатии, причем с произвольным коэффициентом, в подавляющем большинстве блоков незначительно [8]. Малым при сжатии будет не только отклонение СНВ u_1, v_1 от первоначального положения, но и изменение во взаимном расположении векторов u_1, v_1, n-оптимального. Для комплексной количественной оценки полученного качественного заключения был проведен вычислительный эксперимент, в котором анализировались значения углов между векторами u_1 и n-оптимальным, v_1 и n-оптимальным, u_1 и v_1 для ЦИ, первоначально хранимых в формате без потерь, а затем после сжатия с различными коэффициентами качества Q.

В ходе эксперимента для каждого ЦИ в формате TIF, а затем после пересохранения его в JPEG с различными значениями коэффициента качества Q вычислялись средние значения углов между u_1 и v_1 (uv_{sr}), u_1 и n-оптимальным (un_{sr}), v_1 и n-оптимальным (vn_{sr}) по всему изображению. Для i-го ЦИ эти значения обозначались соответственно $uv_{sr}^{(f)}(i)$, $un_{sr}^{(f)}(i)$, $vn_{sr}^{(f)}(i)$, $i = \overline{1,150}$, где верхний индекс f указывает на формат хранения ЦИ (для JPEG-ЦИ он указывает на значение коэффициента качества Q, использованного при сжатии). Результаты проведенного вычислительного эксперимента для наибольшего из рассмотренных возмущающих воздействий ($Q = 2$) отражены на рис. 1, в табл. 1, откуда видно, что для подавляющего большинства ЦИ $uv_{sr}^{(Tif)}(i)$, $un_{sr}^{(Tif)}(i)$, $vn_{sr}^{(Tif)}(i)$ претерпевают при сжатии с $Q = 2$ возмущение, не превосходящее одного градуса (рис. 1), при этом средние значения $abs\left(uv_{sr}^{(Tif)}(i) - uv_{sr}^{(Q2)}(i)\right)$, $abs\left(un_{sr}^{(Tif)}(i) - un_{sr}^{(Q2)}(i)\right)$, $abs\left(vn_{sr}^{(Tif)}(i) - vn_{sr}^{(Q2)}(i)\right)$, $i = \overline{1,150}$, соответственно равны 0.58, 0.45, 0.41. В таблице 1 UV, UN, VN — это средние значения по всем тестируемым изображениям глобальных максимумов гистограмм значений углов между СНВ u_1 и v_1, u_1 и n-оптимальным, v_1 и n-оптимальным соответственно, выраженные в градусах; UV_sr, UN_sr, VN_sr — средние значения по всем тестируемым ЦИ $uv_{sr}^{(f)}(i)$, $un_{sr}^{(f)}(i)$, $vn_{sr}^{(f)}(i)$, $i = \overline{1,150}$, соответственно, выраженные в градусах.

Из таблицы 1 видно, что все рассмотренные в ходе эксперимента характеристики взаимного расположения векторов u_1, v_1, n-оптимального сравнимы для различных форматов и различного качества сжатия. Дополнительным подтверждением этого являются результаты, представленные в таблице 2, полученные в ходе вычислительного эксперимента, в котором тестировалось 300 ЦИ в формате без потерь (TIF), 300 ЦИ в формате JPEG, полученных различными фотокамерами (без привязки к коэффи-

циенту сжатия), 300 изображений в формате JPEG2000, полученных при помощи пересохранения ЦИ из первой группы (TIF) в среде *Adobe* Photoshop с различными коэффициентами качества.

С учетом полученных количественных оценок для возмущений и отклонений предлагается стеганографический алгоритм *SGN*, где в качестве ДИ рассматривается бинарная последовательность $p_1, p_2, ..., p_t$, $p_i \in \{0,1\}$, $i = 1,2,...,t$.

Обозначим *n*-оптимальный вектор n^O. Для погружения 1 бита ДИ используется один 8×8-блок матрицы ЦИ-контейнера.

Погружение ДИ.

Шаг 1. Матрица F размера $m \times n$ контейнера разбивается стандартным образом на 8×8-блоки; B — произвольный блок.

Шаг 2. В каждый блок B погружается очередной бит p_i ДИ:

2.1 Для B строится нормальное сингулярное разложение: $B = U\Sigma V^T$; u_1 и v_1 — левый и правый СНВ блока B соответственно, отвечающие максимальному СНЧ σ_1.

2.2 Погружение p_i:

если $p_i = 1$,

то 2.2.1 $\overline{u}_1 = n^O$, где $\overline{u}_1$ — возмущенный в ходе СП u_1;

2.2.2 Вычисление $\overline{u}_2, ..., \overline{u}_8$ — возмущенных $u_2, ..., u_8$ в процессе приведения левых СНВ к ортонормированному с $\overline{u}_1$ виду.

иначе 2.2.1 $\overline{v}_1 = n^O$, где $\overline{v}_1$ — возмущенный в ходе СП v_1;

2.2.2 Вычисление $\overline{v}_2, ..., \overline{v}_8$ — возмущенных $v_2, ..., v_8$ в процессе приведения правых СНВ к ортонормированному с $\overline{v}_1$ виду.

2.3 Формирование блока $\overline{B}$ СС, отвечающего блоку B контейнера:

если $p_i = 1$,

то $\overline{B} = \overline{U}\Sigma V^T$, где $\overline{U} = \left(n^O, \overline{u}_2, \ldots, \overline{u}_8\right)$,

иначе $\overline{B} = U\Sigma \overline{V}^T$, где $\overline{V} = \left(n^O, \overline{v}_2, \ldots, \overline{v}_8\right)$.

Декодирование ДИ.

Шаг 1. Матрица СС $\overline{F}$ размера $m \times n$ разбивается стандартным образом на 8×8-блоки; $\overline{B}$ — произвольный блок.

Шаг 2. Из каждого блока $\overline{B}$ извлекается очередной бит $\overline{p}_i$ ДИ:

2.1 Для $\overline{B}$ строится нормальное сингулярное разложение: $\overline{B} = \overline{U}\overline{\Sigma}\overline{V}^T$; $\overline{u}_1$ и $\overline{v}_1$ — левый и правый СНВ блока $\overline{B}$ соответственно, отвечающие максимальному СНЧ $\overline{\sigma}_1$.

2.2 Извлечение $\overline{p}_i$. Найти UN_B и VN_B — углы между векторами $\overline{u}_1$, n^O и $\overline{v}_1$, n^O соответственно:

если $UN_B < VN_B$,

то $\overline{p}_i = 1$,

иначе $\overline{p}_i = 0$.

Эффективность работы СА оценивается по объему востановленной информации P в соответствии с соотношением:

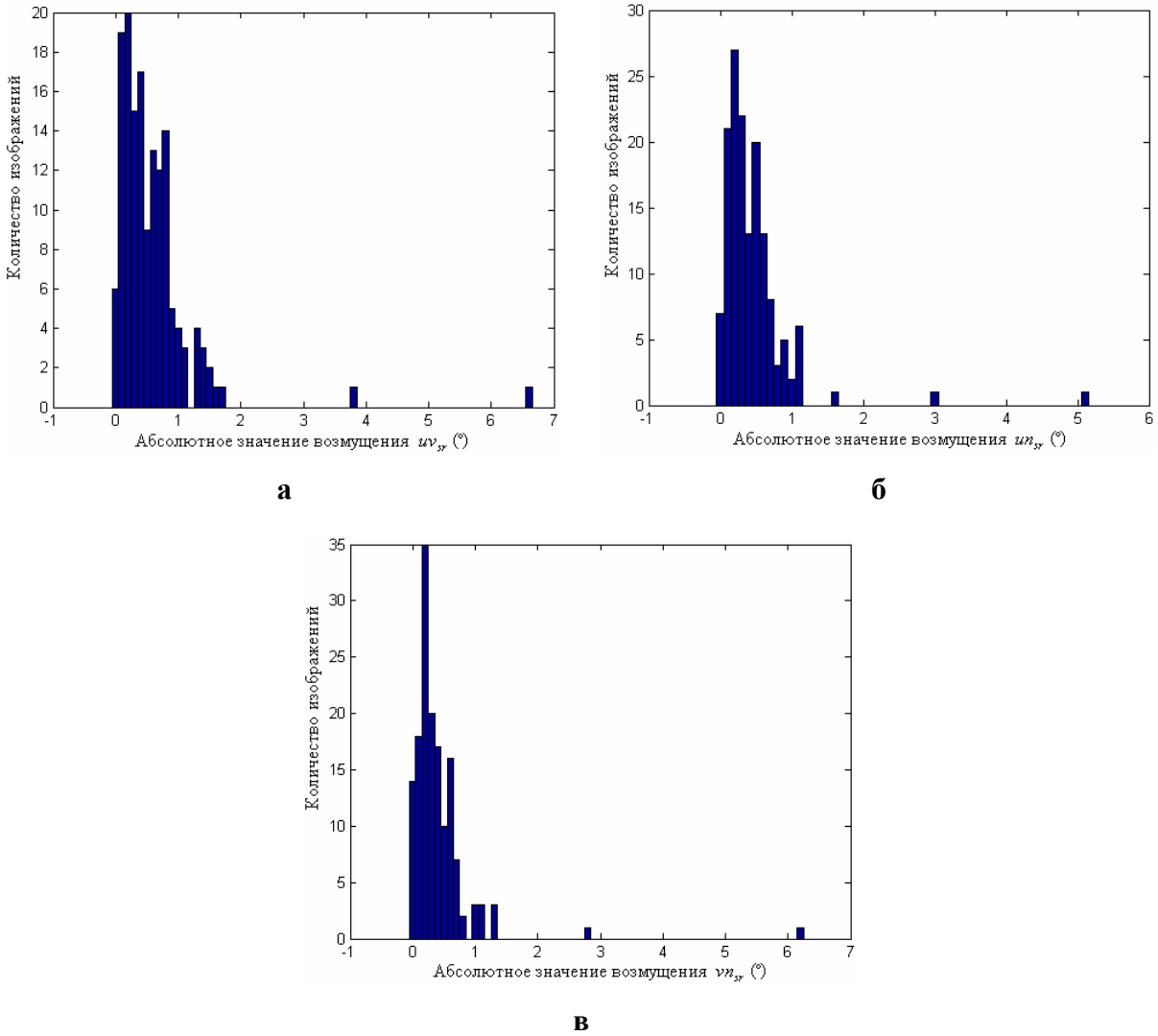
$$P = \frac{t - \sum_{i=1}^{t} p_i \oplus \overline{p}_i}{t} \times 100\%,$$

где

$\oplus$ — операция логического исключающего ИЛИ,

$\overline{p}_1, \overline{p}_2, ..., \overline{p}_t$, $\overline{p}_i \in \{0,1\}$, $i = \overline{1,t}$ — декодированное из СС ДИ.

При организации погружения ДИ на шаге 2.2 возмущение матрицы блока в большинстве случаев не приводило к нарушению надежности восприятия (рис. 2) (за исключением случаев, оговоренных ниже), поскольку возмущение u_1, v_1 при их приравнивании к n^O в подавляющем большинстве блоков незначительно (табл. 1, 2).



а **б**

в

Рис. 1. Результат сжатия ЦИ, хранящегося первоначально без потерь: а – гистограмма значений $abs\left(uv_{sr}^{(Tif)}(i) - uv_{sr}^{(Q2)}(i)\right)$; б – гистограмма значений $abs\left(un_{sr}^{(Tif)}(i) - un_{sr}^{(Q2)}(i)\right)$; в – гистограмма значений $abs\left(vn_{sr}^{(Tif)}(i) - vn_{sr}^{(Q2)}(i)\right)$, $i = \overline{1,150}$

Таблица 1.

Характеристики взаимного расположения СНВ u_1, v_1 и *n*-оптимального вектора

Формат ЦИ		*UV*	*UN*	*VN*	*UV _ sr*	*UN _ sr*	*VN _ sr*
TIF		0.88	0.77	0.66	5.84	4.29	3.76
JPEG	$Q=2$	0.61	0.48	0.31	5.89	4.31	3.74
	$Q=3$	0.65	0.55	0.39	5.91	4.33	3.76
	$Q=4$	0.78	0.58	0.39	5.95	4.36	3.80
	$Q=5$	0.84	0.60	0.51	5.95	4.36	3.81
	$Q=7$	0.85	0.70	0.58	5.88	4.32	3.78
	$Q=9$	0.86	0.74	0.66	5.87	4.32	3.78
	$Q=10$	0.89	0.77	0.69	5.88	4.32	3.72

Таблица 2.

Характеристики взаимного расположения СНВ u_1, v_1 и *n*-оптимального вектора при различных форматах хранения ЦИ

Формат ЦИ	*UV*	*UN*	*VN*	*UV _ sr*	*UN _ sr*	*VN _ sr*
TIF	0.90	0.76	0.64	5.89	4.41	3.87
JPEG	0.94	0.80	0.62	5.97	4.31	3.80
JPEG2000	0.91	0.75	0.61	6.30	5.09	4.53

Организация действий шага 2.2.2 при погружении ДИ может происходить, вообще говоря, различными способами. При проведении вычислительного эксперимента в настоящей работе шаг 2.2.2 конкретизировался следующим образом (рассмотрим на примере матрицы U (рис. 3), где u_i^O — вектор-столбец, ортогональный векторам $\overline{u}_1$ и u_j^O, $j=\overline{2,i-1}$). Обеспечение ортогональности левых СНВ достигалось путем решения системы из 28 линейных алгебраических уравнений с неизвестными x_i, $i=\overline{1,28}$ (рис. 3):

$$\begin{cases}\left(\overline{u}_1, u_j^O\right)=0,\ j=2,..,8,\\ \left(u_i^O, u_j^O\right)=0,\ i=2,..,8,\ j=2,..,i-1,\end{cases} \tag{1}$$

где $(\bullet,\bullet)$ — скалярное произведение векторов-аргуметов. Матрица $\overline{U}$, фигурирующая при формировании матрицы $\overline{B}$ блока СС на шаге 2.3 при погружении ДИ, включает в себя нормализованные векторы-столбцы $\dfrac{u_j^O}{\left\|u_j^O\right\|}$, $j=2,..,8$:

$$\overline{U}=\left(\overline{u}_1 \quad \frac{u_2^O}{\left\|u_2^O\right\|} \quad \frac{u_3^O}{\left\|u_3^O\right\|} \quad \dots \quad \frac{u_8^O}{\left\|u_8^O\right\|}\right)=\left(n^O, \overline{u}_2, \dots, \overline{u}_8\right).$$

а **б**

Рис. 2. Иллюстрация результата СП при помощи алгоритма *SGN*: а – ЦИ-контейнер (формат TIF); б – СС (формат TIF)

$$
\begin{matrix}
\bar{u}_1 = n^{o} & u_2{}^{o} & u_3{}^{o} & u_4{}^{o} & u_5{}^{o} & u_6{}^{o} & u_7{}^{o} & u_8{}^{o} \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow
\end{matrix}
\begin{pmatrix}
1/\sqrt{8} & u_{12} & u_{13} & u_{14} & u_{15} & u_{16} & u_{17} & u_{18} \\
1/\sqrt{8} & u_{22} & u_{23} & u_{24} & u_{25} & u_{26} & u_{27} & x_{22} \\
1/\sqrt{8} & u_{32} & u_{33} & u_{34} & u_{35} & u_{36} & x_{16} & x_{23} \\
1/\sqrt{8} & u_{42} & u_{43} & u_{44} & u_{45} & x_{11} & x_{17} & x_{24} \\
1/\sqrt{8} & u_{52} & u_{53} & u_{54} & x_7 & x_{12} & x_{18} & x_{25} \\
1/\sqrt{8} & u_{62} & u_{63} & x_4 & x_8 & x_{13} & x_{19} & x_{26} \\
1/\sqrt{8} & u_{72} & x_2 & x_5 & x_9 & x_{14} & x_{20} & x_{27} \\
1/\sqrt{8} & x_1 & x_3 & x_6 & x_{10} & x_{15} & x_{21} & x_{28}
\end{pmatrix}
$$

Рис. 3. Возмущенная в процессе СП матрица U

Для проверки эффективности разработанного СА в среде *MathWorks* MATLAB был проведен вычислительный эксперимент, в ходе которого ЦИ размером 1024×1024 пикселя в формате TIF подвергались СП при помощи алгоритма *SGN*. Полученные СС сохранялись первоначально в формате TIF, после чего производилось декодирование ДИ. Затем СС пересохранялись в формат JPEG в среде *Adobe* Photoshop с разными коэффициентами качества Q. Результаты эксперимента для 200 ЦИ приведены в таблице 3.

Таблица 3.

Результаты декодирования ДИ

Формат СС	TIF	JPEG		
		$Q = 10$	$Q = 5$	$Q = 2$
Среднее значение P, %	95.4	95.2	95.0	94.2

Необходимо отметить, что основным возмущающим воздействием для получаемого при помощи *SGN* стеганосообщения, как свидетельствуют результаты эксперимента (табл. 3), является не процесс сжатия, а процессы округлений, происходящие после СП, связанные с введением значений элементов $\overline{B} = \overline{U}\Sigma V^T$ ($\overline{B} = U\Sigma\overline{V}^T$) в диапазон целых значений от 0 до 255, за счет которых и происходят наибольшие из наблюдаемых возмущения углов между $\overline{u}_1$, n^O и $\overline{v}_1$, n^O, приводящие к ошибкам при декодировании ДИ. В последующем процессе сжатия дальнейшее уменьшение объема восстановленной информации практически не происходит. Для иллюстрации в табл. 4 приведены примеры нескольких ЦИ.

Таблица 4.

Объем восстановленной информации при различных форматах СС

№ ЦИ	Формат СС			
	TIF	JPEG		
		Q=10	Q=5	Q=2
1	99.9	99.1	99.1	99.0
2	94.6	93.1	92.8	92.6
3	80.4	80.3	79.7	79.6

Замечание 1. Система (1) может оказаться плохо обусловленной (вырожденной) для некоторых блоков ЦИ-контейнера, что приводит к возникновению артефактов на СС (рис. 4). Как правило, это блоки, отвечающие фоновым областям ЦИ, перепад значений яркости пикселей в их пределах очень незначительный. Такие блоки не используются для погружения ДИ. Как показывает вычислительный эксперимент, количество таких блоков в пределах изображения невелико, и их игнорирование при СП не приводит к значимому снижению скрытой пропускной способности.

Замечание 2. Вычислительная сложность СА *SGN* определяется количеством блоков, получаемых при стандартном разбиении $m \times n$-матрицы F контейнера: $\underline{O}(mn)$, а в случае квадратной матрицы — $\underline{O}(n^2)$.

а **б**

Рис. 4. Пример нарушения надежности восприятия СС, формируемого стеганоалгоритмом *SGN*: а – ЦИ-контейнер (формат TIF); б – СС (формат TIF)

Заключение

В работе на основе установленной sign-нечувствительности к произвольным возмущающим воздействиям, в частности, к атаке сжатием СНВ блоков матрицы ЦИ, отвечающих максимальным СНЧ, разработан новый стеганографический алгоритм, эффективный в условиях сжатия со значительными коэффициентами, обеспечивающий надежность восприятия стеганосообщения. Среднее значение объема восстановленной информации разработанным СА при $Q = 2$ превысило 94%.

Недостатком разработанного алгоритма является малая скрытая пропускная способность канала связи, организуемого при помощи этого алгоритма: $1/64$ бит/пиксель, над проблемой увеличения которой работает в настоящий момент автор.

Список литературы

1. Стеганография, цифровые водяные знаки и стеганоанализ : [монография] / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. — М.: Вузовская книга, 2009. — 220 с.
2. Кобозєва, А.А. Аналіз захищеності інформаційних систем / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко. — К. : Вид. ДУІКТ, 2010. — 316 с.
3. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
4. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
5. Прохожев, Н.Н. Влияние внешних воздействий на DC-коэффициент матрицы дискретно-косинусного преобразования в полутоновых изображениях / Н.Н. Прохожев, О.В. Михайличенко, А.Г. Коробейников // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. — 2008. — Вып. 56. — С. 57–62.
6. Шумейко, А.А. Использование квантования Ллойда-Макса для внедрения цифровых водяных знаков / А.А. Шумейко, А.И. Пасько, Т.Н. Тищенко // Інформаційна безпека. — 2010. — № 2(4). — С. 101–108.
7. Кобозева, А.А. Анализ информационной безопасности: монография / А.А. Кобозева, В.А. Хорошко. — К.: ГУИКТ, 2009. — 251 с.
8. Кобозева, А.А. Нечувствительность стеганосообщения к сжатию и формальные достаточные условия ее обеспечения / А.А. Кобозева, М.А. Мельник // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. — 2012. — Вип. 38. — С. 193–203.
9. Гантмахер, Ф.Р. Теория матриц [Текст] : монография / Ф.Р. Гантмахер. — 5-е изд. — М. : Физматлит, 2004. — 559 с.
10. Кобозева, А.А. Векторная SIGN-чувствительность как основа геометрической модели системы защиты информации / А.А. Кобозева, В.А. Хорошко // Захист інформації. — 2008. — Том 10, № 3(40). — С. 49–57.
11. Зорило, В.В. Анализ особенностей сингулярных чисел матриц цифровых изображений при разных степенях сжатия для выявления фотомонтажа / В.В. Зорило, А.А.Кобозева // Захист інформації. — 2010. — Том 12, № 3(48). — С. 34–41.

SIGN-НЕЧУТЛИВІСТЬ СИНГУЛЯРНИХ ВЕКТОРІВ МАТРИЦІ ЗОБРАЖЕННЯ ЯК ОСНОВА СТЕГАНОАЛГОРИТМУ, СТІЙКОГО ДО СТИСКУ

М.О. Мельник

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: ritochek@yandex.ru

У роботі на основі sign-нечутливості, що забезпечує нечутливість сингулярних векторів стандартних блоків матриці цифрового зображення, що відповідають максимальним сингулярними числами, до довільних збурюючих дій, розроблений поліноміальний ступеня 2 стеганографічний алгоритм, стійкий до стиснення із значними коефіцієнтами. Наведено результати обчислювального експерименту, що підтверджують ефективність запропонованого алгоритму.
Ключові слова: сингулярний вектор, сингулярне число, sign-чутливість, збурююча дія, стиск, матриця

SINGULAR VECTORS SIGN-INSENSITIVE AS BASIS TO DEVELOPMENT COMPRESSION-STABLE STEGANOGRAPHIC ALGORITHM

Margaret A. Melnik

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: ritochek@yandex.ru

The paper focuses on new steganographic algorithm development. Proposed algorithm is stable to compression, including high rate compression, and based on singular vectors insensitive of image matrix blocks which corresponding to maximal singular values. Algorithm is polynomial of degree 2. The results of numerical experiments confirm the efficiency of the proposed algorithm.
Keywords: singular vector, singular value, sign-sensitivity, disturbance, compression, matrix

УДК 519.876.5

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 2, pp. 156-162

АНАЛІЗ МОЖЛИВОСТЕЙ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ СКЛАДНИХ РАДІОТЕХНІЧНИХ СИСТЕМ

С.В. Гахович[1], О.В. Мірошніченко[1], М.М. Охрамович[1], Т.В. Савченко[2]

[1] Військовий інститут Київського національного університету імені Тараса Шевченка,
вул. Ломоносова, 81, Київ, 03680, Україна; e-mail: gahh@bigmir.net
[2] Київський національний торговельно-економічний університет,
вул. Кіото, 19, Київ, 02156, Україна; e-mail: sv_t@ukr.net

У статті розглянуті можливості імітаційного моделювання складних радіотехнічних систем у програмному середовищі Simulink математичного пакету MATLAB на прикладі створення програмної імітаційної моделі радіопередавального пристрою радіолокатора.

Ключові слова: імітаційна модель, радіотехнічна система, передавач

Вступ

Імітаційне моделювання – це метод дослідження, при якому досліджувана система замінюється моделлю, що з достатньою точністю описує реальну систему, з якою проводяться експерименти з метою отримання інформації про цю систему. Експериментування з моделлю називають імітацією (імітація – це дослідження суті явища, не вдаючись до експериментів на реальному об’єкті).

Імітаційне моделювання – це окремий випадок математичного моделювання. Існує клас об'єктів, для яких з різних причин не розроблені аналітичні моделі, або не розроблені методи вирішення отриманої моделі. В цьому випадку аналітична модель замінюється імітатором або імітаційної моделлю.

Математичне моделювання ґрунтується на досягненнях математики – як класичної, так і новітньої комп’ютерної, орієнтованої на виконання обчислень за допомогою сучасних комп’ютерів та прикладних математичних програм для імітаційного моделювання [1–3]. У статті розглянуті можливості цифрового моделювання складних радіотехнічних систем за допомогою математичного пакету *MathWorks* MATLAB.

Програма Simulink є додатком до пакету MATLAB. При моделюванні з використанням Simulink реалізується принцип візуального програмування, відповідно до якого, користувач на екрані з бібліотеки стандартних блоків створює модель пристрою і здійснює розрахунки. При цьому, на відміну від класичних способів моделювання, користувачеві не потрібно досконально вивчати мову програмування і чисельні методи математики, а достатньо загальних знань потрібних при роботі на комп’ютері і, природно, знань тієї предметної області в якій він працює [4].

Чим складніше проектований об’єкт, тим, як правило, важливіша роль моделювання в його вивченні і створенні.

Реальна користь від моделювання може бути отримана при виконанні двох головних умов:

- модель повинна бути адекватною оригіналу в тому сенсі, що повинна з необхідною точністю відображати характеристики оригіналу;

▪ модель повинна усувати проблеми, пов'язані з фізичним вимірюванням сигналів або характеристик оригіналу [5, 6].

Мета статті і постановка задачі дослідження

Дослідження радіотехнічних систем, зокрема параметрів зондуючого сигналу радіолокаційної станції (тим більше дослідження змін параметрів сигналу зі зміною величин, що на нього впливають) достатньо складна задача. Це пов'язано зі складністю апаратури, її вартістю і характеристик самого сигналу. Наприклад для сучасних радіолокаторів імпульсна потужність зондуючого сигналу може знаходитись у межах порядку кілька сотень кіловат – одиниці мегават, сигнал може мати складну структуру, частоти таких сигналів знаходиться в межах одиниць – десятків гигагерць [7]. Вимірювання параметрів таких сигналів проводиться непрямими методами з похибкою, яка граничить з допустимою для інженерних розрахунків. Для дослідження саме таких складних систем доцільно використовувати імітаційне моделювання. Розглянемо можливості програмного середовища Simulink на прикладі побудови імітаційної моделі пристрою формування сигналів передавача реалізованого за схемою задавальний генератор – підсилювач потужності.

Виклад основного матеріалу дослідження

Для прикладу розглянемо роботу радіолокатора, який працює в режимі істинної внутрішньої когерентності. Загальний принцип побудови таких радіолокаторів полягає в наявності двох високостабільних генераторів безперервних коливань: генератора частоти гетеродину ($f_г$) та генератора проміжної частоти ($f_{пч}$), що одночасно приймають участь у формуванні зондуючих сигналів та обробці прийнятих сигналів відлуння [7].

При формуванні зондуючих сигналів в результаті зшивання частот двох генераторів виникає безперервне коливання несучої частоти $f_{нес} = f_г + f_{пч}$ періодичні «вирізки» з якої і використовується у якості зондуючого сигналу. Розглянемо передавальну систему радіолокатора, де в якості зондуючого використовується складний 4-х частотний сигнал. Його формування його здійснюється у 4-х паралельних каналах збуджувача передавача, для чого використовується 4 гетеродина. Перед поданням на вихідний підсилювач 4 радіоімпульси об'єднуються в один складний 4-х частотний сигнал. Спрощена структурна схема пристрою формування сигналів передавача показана на рис. 1.

Пристрій формування сигналів передавача формує радіоімпульси на чотирьох частотах. Формування радіоімпульсів відбувається у чотирьох однакових (по схемному рішення) підканалах. В якості джерела високостабільних сигналів проміжної частоти $f_{пч}$ використовуються високостабільні кварцові генератори. Сигнали управління роботою передавача надходять з хронізатора у вигляді імпульсів запуску відповідного каналу І3.1 – І3.4.

Канал формування гетеродинної напруги складається з кварцового генератора з виходу якого безперервний сигнал поступає на підсилювач-помножувач де відбувається підсилення його по потужності і підвищення частоти до значення: $f_{г1}$, $f_{г2}$, $f_{г3}$, $f_{г4}$ відповідно кожному частотному каналу. Одна третина потужності отриманого сигналу в якості генераторної напруги поступає на прийомну систему для обробки сигналів відлуння, а лишок потужності на змішувач передавача. Одночасно на цей змішувач (в кожному каналі) надходять радіоімпульси («вирізки») з високостабільної напруги проміжної частоти $f_{пч}$, що формуються у блоці формування імпульсів проміжної частоти. На виході змішувача за допомогою смуго-пропускного фільтру отримаємо

сумарну частоту $f_н = f_г + f_{пч}$, що є вихідною (несучою) частотою передавального пристрою.

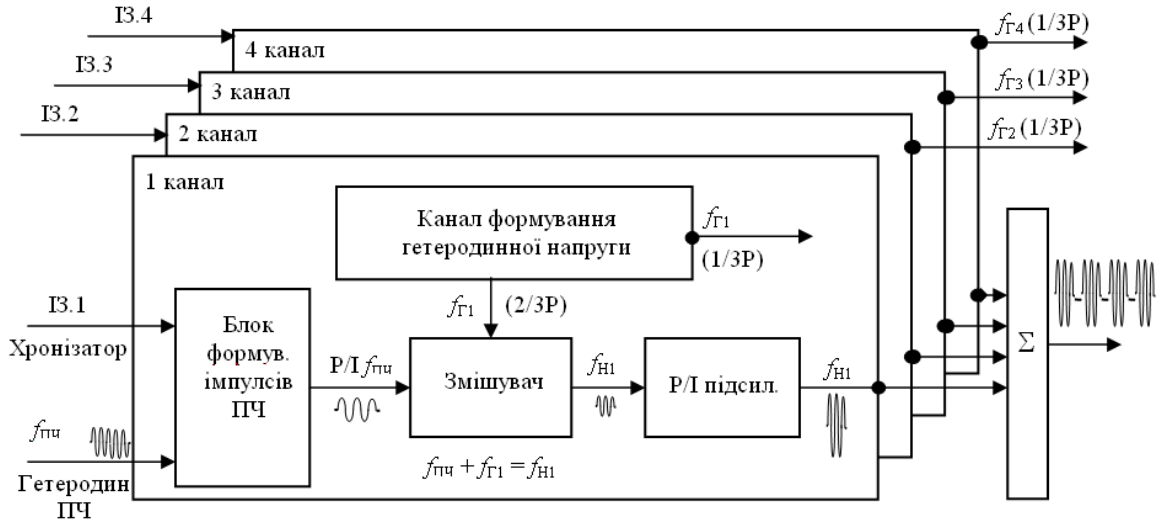


Рис. 1. Спрощена структурна схема пристрою формування сигналів передавача

Сформовані змішувачами і підсилені у підсилювачах, сигнали на частотах $f_{Н1}$, $f_{Н2}$, $f_{Н3}$, $f_{Н4}$ надходять на частотний суматор, де об`єднуються у один складний чотирьох частотний сигнал у вигляді когерентної послідовності радіоімпульсів.

Відповідно до принципу роботи пристрою формування сигналів передавача за допомогою математичного програмного пакету *MathWorks* MATLAB необхідно сформувати потужний складний чотирьох частотний сигнал, який складається з безперервний гармонійних сигналів генератора проміжної частоти та гетеродинів. Імітаційна модель першого каналу пристрою формування сигналів передавача показана на рис. 2.

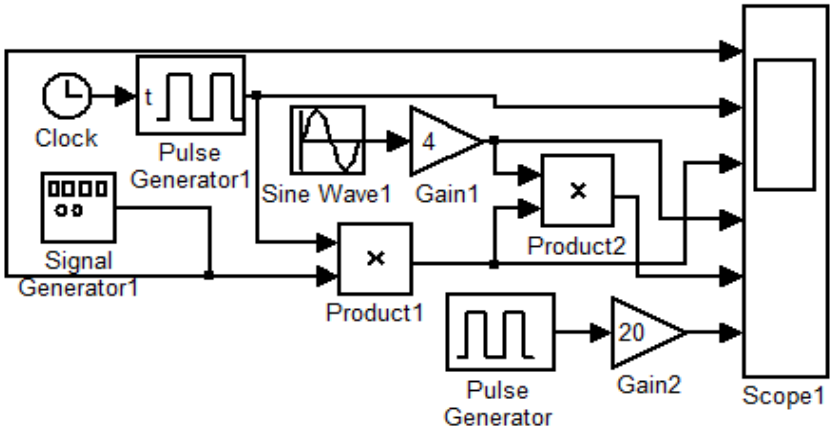


Рис. 2. Імітаційна модель 1-го каналу пристрою формування сигналів передавача

В якості імпульсів запуску (ІЗ.1), які находять із хронізатору, використовується джерело часового сигналу *Clock* сигнали якого запускають імпульсний генератор *Pulse Generator 1*, що формує прямокутний імпульс тривалістю 10 мкс. Цей імпульс одно-

часно з сигналом проміжної частоти $f_{\text{пч}}$ (формується *Signal Generator 1*) надходить на блок помножувача *Product 1* з виходу якого виходять «вирізки» сигналу на проміжній частоті з необхідною тривалістю, яка задається генератором *Pulse Generator 1*. Зазначена схема імітує роботу формувача блоку формування радіоімпульсів проміжної частоти. Сигнал гетеродину $f_{\text{г}}$ формується джерелом синусоїдального сигналу *Sine Wave 1* та підсилюється підсилювачем *Gain 1* (імітує роботу каналу формування гетеродинної напруги) і разом з «вирізкою» сигналу на проміжній частоті $f_{\text{пч}}$ надходить на блок помножувача *Product 2* (імітує роботу змішувача), з виходу якого знімається сформований імпульс на сумарній частоті $f_{\text{н}}$, що далі підсилюється і випромінюється у простір в якості зондуючого сигналу відповідного каналу. Робота радіоімпульсного підсилювача в імітаційній моделі показана блоками *Pulse Generator* та *Gain 2*.

Канал формування гетеродинної напруги складається з когерентного гетеродину, підсилювача та підсилювача-помножувача. В імітаційній моделі канал задається одним джерелом синусоїдального сигналу *Sine Wave 1* та підсилювачем *Gain 1* з параметрами, що відповідають формуванню на виході безперервного коливання необхідної частоти та амплітуди. В зазначеній імітації не враховано:

- вплив власних шумів радіоелементів;
- довгочасна відносна нестабільність несучої частоти;
- робота феритових вентилів, які служать для захисту передавача від відбитих хвиль.

Зазначені обмеження в цілому не суттєво впливають на кінцевий результат, тому що розглянутий радіолокатор працює у режимі істинної внутрішньої когерентності і сформований сигнал (з перекручуваннями викликаними власними шумами та нестабільністю частоти) приймає участь в обробці ідентичного прийнятого сигналу і зазначені похибки нівелюються. Феритові вентилі, як елементи захисту, наряду з пристроями контролю та сигналізації є допоміжними пристроями, які не впливають на роботу загальної імітаційної моделі і призначені для вирішення другорядних задач контролю функціонування, роботи та пошуку несправностей. Тому спрощення, які використанні в імітаційній моделі, допустимі, і в цілому модель адекватна існуючим технічним рішенням.

Загальна імітаційна модель 4-х канального пристрою формування сигналів передавача показана на рис. 3.

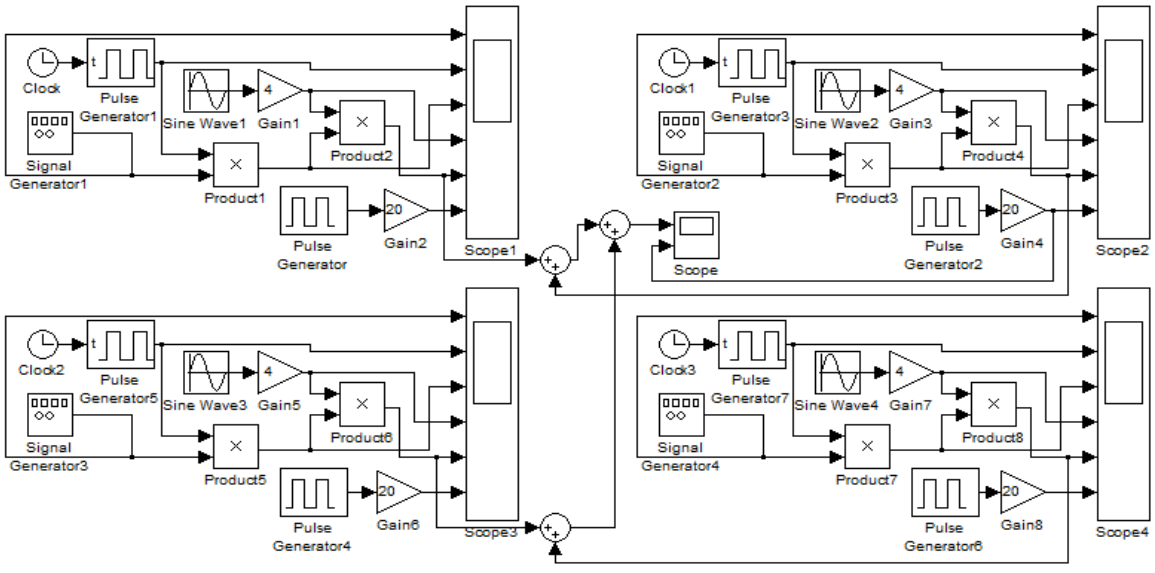


Рис. 3. Імітаційна модель 4-х канального пристрою формування сигналів передавача

У цій моделі присутні чотири ідентичних канали вихідні сигнали яких поєднуються за допомогою трьох суматорів (імітують роботу вихідного чотирьохканального суматора). Осцилограми сигналів кожного каналу відображені на відповідних осцилографах *Scope 1* (*2, 3, 4*), загальний вигляд (осцилограма *Scope*) сформованого чотирьох частотного сигналу та модулюючого імпульсу модулятора показані на рис. 4.

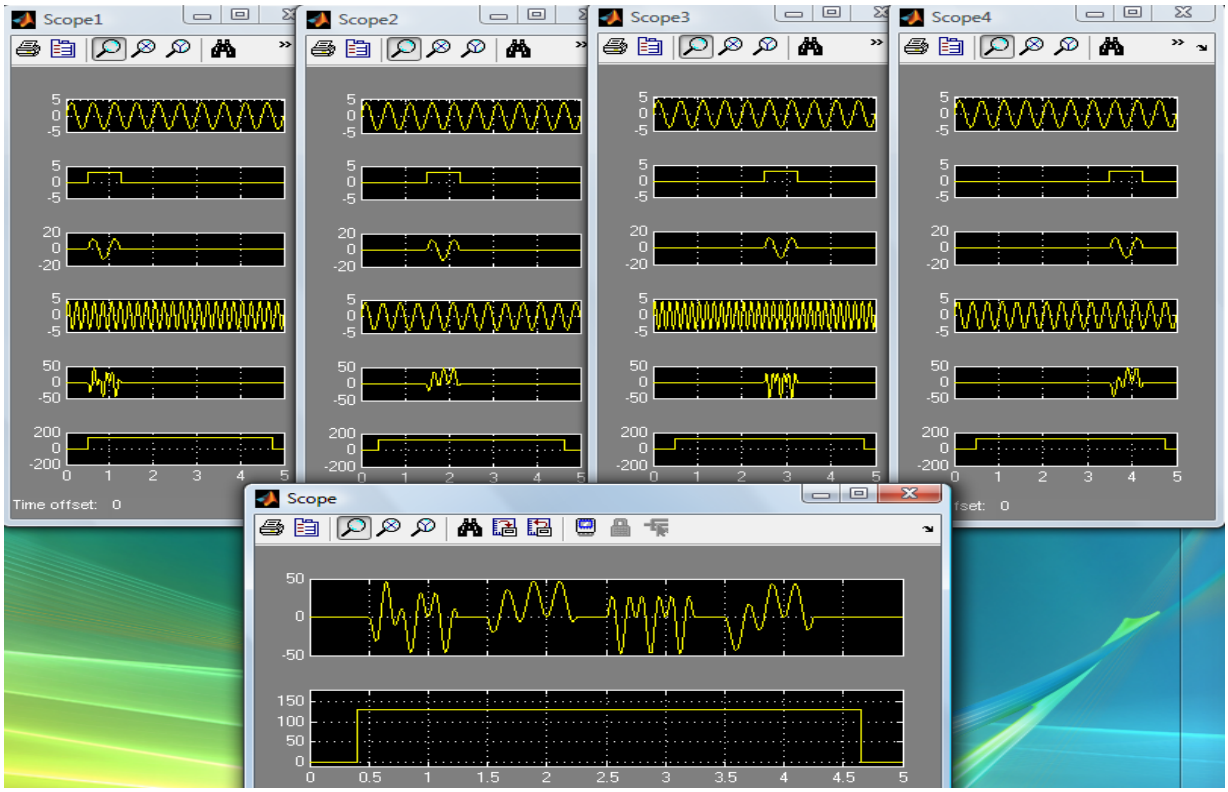


Рис. 4. Осцилограми вихідних сигналів передавача радіолокатора

Отримані результати

За допомогою програми Simulink, яка входить до математичного пакету MATLAB, вирішена практична задача по розробці імітаційної моделі радіотехнічної системи. Отримані результати дозволяють зробити висновок про можливість розробки загальної структурної імітаційної моделі радіолокатора, яка дасть змогу дослідити зміни параметрів функціонування радіолокатора при зміні алгоритмів роботи окремих функціональних пристроїв. Імітаційна модель наглядна, дозволяє оцінити значення вихідних параметрів, має змогу змінювати параметрів сигналів в широких межах, а також дає можливості для експериментування з використанням нових технічних рішень.

Адекватність імітаційної моделі підтверджується використанням апробованого математичного апарату та збіганням отриманих результатів з практичними (за окремими показниками характеристик вихідних сигналів та алгоритму роботи).

Переваги даної імітаційної моделі полягають у достатній простоті реалізації, можливості швидко та гнучко змінювати характеристики пристроїв та параметрів сигналів. Широкий набір заготовлених імітаційних пристроїв та можливість корегувати функції їх роботи дозволяють інженеру вирішувати завдання високої складності, безпосередньо у часі та на будь-якому кроці отримувати контрольні данні для проведення досліджень.

Висновки

Розроблена імітаційна модель частини передавального пристрою радіолокатора показала можливість використання програмного імітатора Simulink математичного пакету MATLAB для вирішення інженерних задач по моделюванню складних радіотехнічних систем. Імітаційна модель з достатньою адекватністю описує основні якості об'єкту, що моделюється, наглядна і дозволяє досліджувати часові параметри сигналів на виході будь-якого пристрою моделі. Її використання дозволяє суттєво скоротити витрати часу та коштів при дослідженнях можливості вдосконалення системи або розробки нових радіотехнічних систем, які будуть відповідати поставленим завданням, що висуваються до нових зразків радіотехнічних систем.

Список літератури

1. Дьяконов, В.П. Компьютерная математика [Текст] : теория и практика / В.П. Дьяконов ; Российская Ассоциация Издателей компьютерной литературы. — М. : Нолидж, 2001. — 1296 с.
2. Дьяконов, В.П. MATLAB. Анализ, идентификация и моделирование систем [Текст] : спец. справ. / В.П. Дьяконов, В. Круглов. — СПб. : Питер, 2002. — 444 с.
3. Дьяконов, В.П. MATLAB и SIMULINK для радиоинженеров [Текст] / В.П. Дьяконов. — М. : ДМК Пресс, 2011. — 976 с.
4. Черных, И.В. Моделирование электротехнических устройств в MATLAB, SimPowerSystems и Simulink [Текст] / И.В. Черных. — М. : ДМК Пресс ; М. ; СПб. ; Н. Новгород [и др.] : Питер, 2008. — 288 с.
5. Бенькович, Е.С. Практическое моделирование динамических систем [Текст] / Е.С. Бенькович, Ю.Б. Колесов, Ю.Б. Сениченков. — СПб.: БХВ Петербург, 2002. — 464 с.
6. Шеннон, Р. Имитационное моделирование систем – искусство и наука / Р. Шеннон ; пер. с англ. под ред. Е.К. Масловского. — М. : Мир, 1978. — 418 с.
7. Довідник з протиповітряної оборони / А.Я. Торопчін, І.О. Романенко, Ю.Г. Даник, Р.Е. Пащенко та ін. — К. : МО України, Х : ХВУ, 2003. — 368 с.

АНАЛИЗ ВОЗМОЖНОСТЕЙ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ СЛОЖНЫХ РАДИОТЕХНИЧЕСКИХ СИСТЕМ

С.В. Гахович[1], О.В. Мирошниченко[1], М.Н. Охрамович[1], Т.В. Савченко[2]

[1] Военный институт Киевского национального университета имени Тараса Шевченко,
ул. Ломоносова, 81, Киев, 03680, Украина; e-mail: gahh@bigmir.net
[2] Киевский национальный торгово-экономический университет,
ул. Киото, 19, Киев, 02156, Украина; e-mail: sv_t@ukr.net

В статье рассмотрены возможности имитационного моделирования сложных радиотехнических систем в программной среде Simulink математического пакета MATLAB на примере создания программной имитационной модели радиопередающего устройства радиолокатора.
Ключевые слова: имитационная модель, радиотехническая система, передатчик

ANALYSIS OF OPPORTUNITIES FOR SIMULATION OF COMPLEX RADIO SYSTEMS

Sergey V. Gakhovich[1], Oleg V. Miroshnichenko[1], Myhaylo M. Okhramovich[1], Tatiana V. Savchenko[2]

[1] Military Institute, Taras Shevchenko National University of Kyiv,
81 Lomonosov str., Kyiv, 03680, Ukraine; e-mail: gahh@bigmir.net
[2] Kyiv National University of Trade and Economics,
19 Kyoto str., Kyiv, 02156, Ukraine; e-mail: sv_t@ukr.net

This paper examines the possibilities for simulation of complex radio systems. Modelling and simulation is developed in Simulink environment and validated through experimental data. In this paper we offer example to show how simple simulation model of radar transmitter.
Keywords: simulation model, radio system, transmitter

УДК 004.932.2

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 2, pp. 163-168

НОВАЯ КЛАССИФИКАЦИЯ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

Е.В. Нариманова, Е.А. Трифонова

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: semejka@ua.fm

Предложена новая классификация методов защиты информации с учетом методов проверки целостности цифровых сигналов, которые на сегодняшний день вызывают наибольший интерес, однако не имеют своего места в рамках методов и средств защиты информации.

Ключевые слова: классификация, методы защиты информации, методы проверки целостности, методы активной защиты информации, методы пассивной защиты информации

Введение

Процесс внедрения новых информационных технологий во все сферы жизни общества немыслим без решения вопросов информационной безопасности, которая структурируется в совершенно разных, но связанных между собой аспектах [1, 2] (рис. 1).

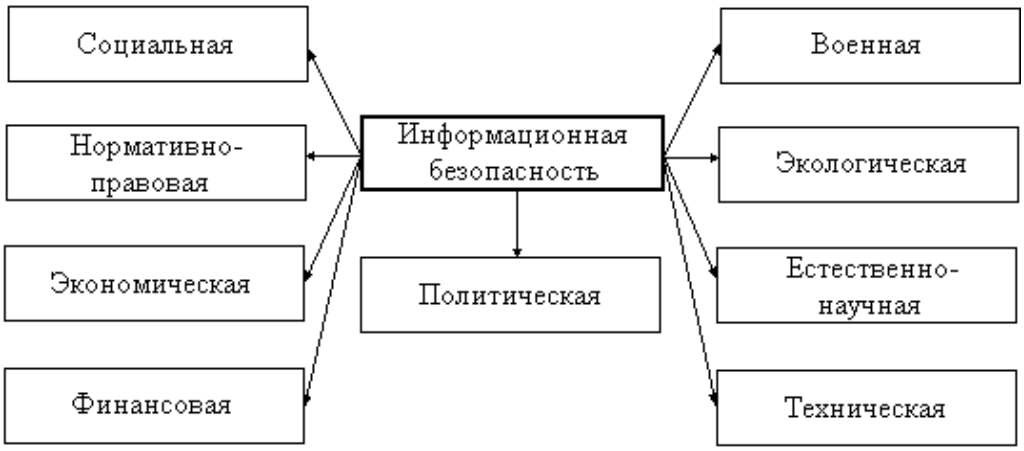


Рис. 1. Аспекты проблемы информационной безопасности

Широкомасштабное использование вычислительной техники и телекоммуникационных систем, переход к безбумажной технологии, увеличение объемов обрабатываемой информации и расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационных систем, к их высокой уязвимости. В современных условиях возникает необходимость защиты не только государственной и военной, но и промышленной, коммерческой и финансовой тайн. Защита информации в целом, в том числе защита информации в автоматизированных системах, становится все более

актуальной и сложной проблемой, для решения которой необходимо построение общего системного комплексного подхода к защите информации.

Современная концепция комплексной защиты согласуется с идеями, высказанными еще в 1986 г. в [3], где впервые в отечественной печати затрагиваются вопросы перспектив развития теории защиты, принципиальные положения которой сформулированы чуть позже в [4], где комплексность защиты информации строго обоснованно ставится на первое место.

В [1, 2] представлен систематизированный обзор современного состояния и путей развития методов и средств защиты информации. Используемый для этого единый системно-концептуальный подход, в рамках которого проводится выделение в предметной области защиты информации трех иерархий: структурной, причинно-следственной и функциональной, рассматривающий и анализирующий все значительные факторы не отдельно, а как систему, приводит к выработке совокупности взглядов и оценок для общего случая на сущность проблем и общих решений. Одной из системообразующих задач является обоснованный выбор требуемого уровня защиты информации, поскольку как занижение, так и завышение уровня неизбежно ведет к потерям. В связи с этим чрезвычайно значимой является систематизация и обоснование создания условий, необходимых для оптимальной реализации концепции защиты [1, 2].

Системно-концептуальный подход, используемый в [1], получил дальнейшее развитие в [5], где выдвигается единая концепция защиты, основанная на комплексном применении всех имеющихся методов и средств, определяются основные требования к комплексным системам защиты информации, среди которых:

- использование комплекса программно-технических средств и организационных мер;
- надежность, производительность, конфигурируемость;
- экономическая целесообразность;
- возможность совершенствования;
- обеспечение разграничения доступа к конфиденциальной информации с отвлечением нарушителя на ложную информацию;
- взаимодействие с незащищенными компьютерными сетями по установленным для этого правилам разграничения доступа;
- обеспечение проведения учета и расследования случаев нарушения безопасности информации в компьютерных сетях и т.д.

Дальнейшее совершенствование теории защиты очевидно связано с учетом новых обстоятельств, характерных для современного периода развития информатизации общества:

- наблюдаемые в последние годы тенденции в развитии информационных технологий ведут к появлению качественно новых (информационных) форм борьбы, в том числе и на межгосударственном уровне. В силу этого все большую актуальность приобретает не только защита информации, но и защита людей и технических (главным образом, электронных) систем от разрушающего воздействия информации, в связи с чем формируется задача обеспечения информационной безопасности как органической совокупности задач защиты информации и защиты от информации;
- с самого начала регулярного использования автоматизированных технологий обработки информации актуальной является задача обеспечения требуемого качества информации. С течением времени актуальность данной задачи возрастает, а сама задача усложняется;
- основное внимание на новом этапе развития теории защиты информации должно быть уделено совершенствованию научно-методологического базиса и инструментальных средств, обеспечивающих решение любых возникающих задач на регулярной основе.

Углубленное изучение проблемы совершенствования научно-методологического базиса теории защиты информации привело к выводу, что уже в настоящее время и в перспективе решение проблем защиты вне органической связи с решением более общих проблем (информационных технологий, информатизации общества и т.д.) может привести к неадекватным результатам.

Цель стать и постановка заданий

До недавнего времени комплексные системы защиты информации были ориентированы на защиту информации, которая создается, редактируется и передается непосредственно в самой системе. Однако, существование и функционирование любой системы невозможно без коммуникации с внешней средой и другими системами. Таким образом, защищенность информации в самой системе будет зависеть от достоверности и целостности информации, поступающей извне. До недавнего времени методы проверки целостности не были учтены при построении классификации методов защиты информации.

Целью данной работы является построение новой классификации методов защиты информации с учетом методов проверки целостности цифровых сигналов.

Для достижения поставленной цели необходимо решить следующие задачи:

1) Рассмотреть существующие классификации методов защиты информации;
2) Определить основание для классификации на каждом уровне;
3) Провести классификацию методов проверки целостности цифровых сигналов.

Основная часть

Для решения задач защиты информации (ЗИ) существует целый ряд методов, которые, по способу их реализации были классифицированы следующим образом: организационные, технические, криптографические и программные [1,2].

Организационные методы защиты информации (МЗИ), в свою очередь, были разделены на законодательные [5–7], административные [8] и морально-этические методы, которые направлены на: использование законодательных актов, регламентирующих права и обязанности физических и юридических лиц, а также государства в области ЗИ; организацию соответствующего режима секретности, пропускного и внутреннего режима на объекте; создание и поддержание на объекте моральной атмосферы, в которой нарушение регламентированных правил поведения оценивалось бы большинством сотрудников резко негативно [1].

Технические методы включают в себя применение электронных и других устройств для ЗИ [9].

В *криптографических* методах используется шифрование и кодирование для сокрытия обрабатываемой и передаваемой информации от несанкционированного доступа [10,11].

Программные методы используют программные средства разграничения доступа к информации [5].

Представленные методы защиты информации нацелены на сохранение основных категорий информации – целостности, доступности, конфиденциальности, достоверности. Такие методы назовем методами *активной* защиты информации (МАЗИ).

В последние годы благодаря широкому распространению всевозможных средств (бытовых и специальных) фиксации и хранения фото-, видео- и аудиоинформации в распоряжении органов дознания, следствия и суда часто оказываются фотографии, видео- и аудиозаписи, которые могут являться доказательствами по уголовному делу.

Все чаще возникают следственные ситуации, в которых появляется необходимость в производстве экспертизы предоставленных материалов [12].

Для решения подобных задач применяются другие методы защиты информации (МЗИ), целью работы которых (в отличие от МАЗИ) является обоснованная констатация факта наличия или отсутствия нарушения одной или нескольких категорий информации, чаще всего целостности. Назовем их методами *пассивной* ЗИ (МПЗИ).

В качестве основания на первом уровне новой классификации предлагается использовать цель использования МЗИ, на втором – способ реализации (способ достижения цели) МЗИ. Схематически предложенная классификация методов защиты информации представлена на рисунке 2.

Методы защиты информации первоначально можно классифицировать по цели их использования на методы активной и пассивной защиты. Целью методов активной защиты информации является сохранение всех категорий информации. Методы пассивной защиты информации нацелены на то, чтобы дать ответ, было ли произведено преднамеренное нарушение какой-либо категории информации.

По способу реализации МАЗИ можно классифицировать в соответствии с [1, 2] на организационные, технические, криптографические и программные. МПЗИ по способу их реализации можно разделить на методы экспертной оценки, программно-технические и программные.

Методы *экспертной* оценки используют визуальное или акустическое оценивание информации специалистом. Главным недостатком методов экспертной оценки является наличие человеческого фактора.

Программно-технические МПЗИ основываются на знании специфических особенностей устройств аудио-, видео- или фотофиксации и (или) воздействия каких-либо внешних факторов на проведение записи.

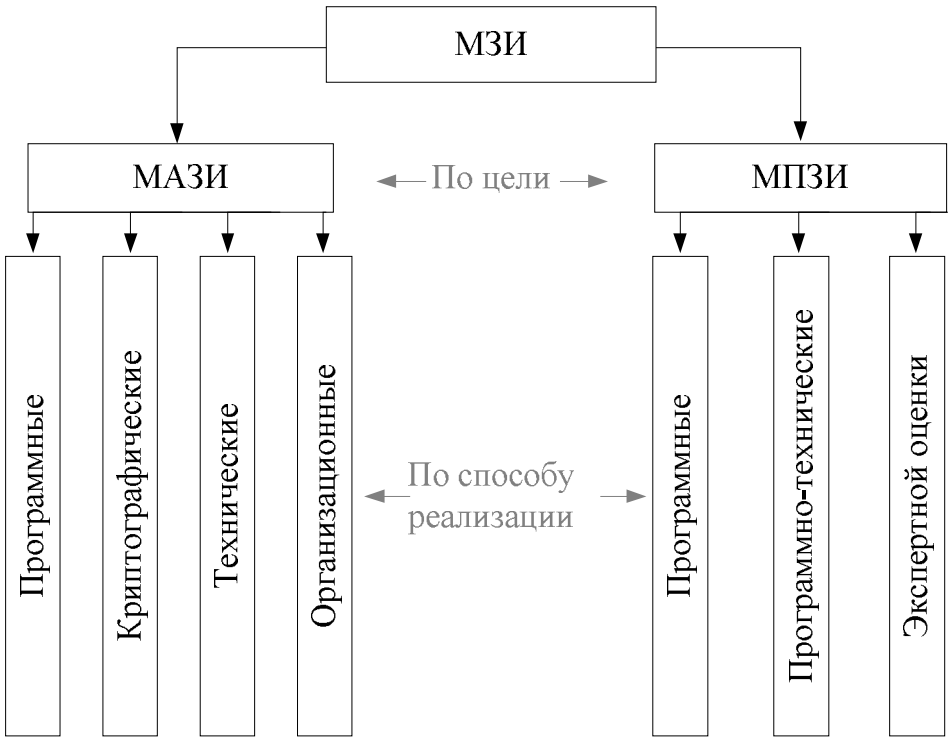


Рис. 2. Новая классификация методов защиты информации

Программные методы ЗИ анализируют лишь цифровую форму представления самого сигнала [13, 14], а поэтому не зависят от технических характеристик устройств или человеческого фактора, как в программно-технических методах и методах экспертного оценивания.

Выводы

В работе построена новая классификация МЗИ, которая более полно отражает существующие на сегодняшний день методы защиты информации, дает системное представление о способах их реализации и позволяет определить место методов проверки целостности цифровых сигналов среди всех остальных методов.

Предложенная классификация может быть полезна при изучении существующих и разработке новых методов и средств защиты информации.

Список литературы

1. Хорошко, В.А. Методы и средства защиты информации [Текст] : научное издание / В.А. Хорошко, А.А. Чекатков; Ред. Ю.С. Ковтанюк. — К. : ЮНИОР, 2003. — 505 с.
2. Ленков, С.В. Методы и средства защиты информации: в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. — К.: Арий, 2008 — . — Т.2: Информационная безопасность. — 2008. — 344 с.
3. Мамиконов, А.Г. Достоверность, защита и резервирование информации в АСУ [Текст] / А.Г. Мамиконов, В.В. Кульба, А.Б. Шелков. — М. : Энергоатомиздат, 1986. — 303 с.
4. Тихонов, А.Н. О состоянии работ по совершенствованию подготовки кадров по проблеме информационной безопасности / А.Н. Тихонов // Безопасность информационных технологий. — 1995. — № 4. — С. 43–52.
5. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах [Текст] : учебное пособие для студентов вузов, обучающихся по спец. «Информатика и вычислительная техника» / П.Б. Хорев. — 2-е изд., стер. — М. : Изд. центр «Академия», 2006. — 256 с.
6. Чумарин, И.Г. Тайна предприятия: что и как защищать : учебное пособие / И.Г. Чумарин. — Санкт-Петербург : ДНК, 2001. — 160 с.
7. Стрельцов, А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы [Текст] : монография / А.А. Стрельцов ; Под ред. В.А. Садовничего, В.П. Шерстюка. — М. : МЦНМО, 2002. — 289 с.
8. Степанов, Е.А. Информационная безопасность и защита информации [Текст] : учеб. пособие / Е.А. Степанов, И.К. Корнеев. — М. : Инфра-М, 2001. — 302 с.
9. Хорев, П.Б. Способы и средства защиты информации / П.Б. Хорев. — М.: МО РФ, 2000. — 316 с.
10. Фергюсон, Н. Практическая криптография [Текст] : монография / Н. Фергюсон, Б. Шнайер ; Пер. с англ. Н.Н. Селиной. — М. и др. : ИД Вильямс : Диалектика, 2005. — 421 с.
11. Столингс, В. Криптография и защита сетей [Текст] : принципы и практика / Пер. с англ. А.Г. Сивака, А.А. Шпака; Под ред. А.Г. Сивака. — 2-е изд. — М. СПб. Киев : Вильямс, 2001. — 672 с.
12. Оленин, Г.В. Экспертиза цифровой аудио- и видеозаписи. Применение в следственной практике устройств цифровой фиксации аудио- и видеоинформации / Г.В. Оленин // Эксперт-криминалист. — 2009. — № 2. — С. 21–24.
13. Нариманова, Е.В. Исследование эффекта двойного квантования и его использование при обнаружении фальсификации ЦИ / Е.В. Нариманова // Вісник Східноукраїнського національного університету ім. В. Даля. — 2008. — № 8(126), Ч. 1. — С. 47–55.
14. Нариманова, Е.В. Практическое использование DQ-эффекта для построения универсального метода обнаружения фальсификации ЦС / Е.В. Нариманова // Вісник Східноукраїнського національного університету ім. В. Даля. — 2010. — № 9(151), Ч. 1. — С. 80–85.

НОВА КЛАСИФІКАЦІЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

О.В. Наріманова, К.О. Трифонова

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: semejka@ua.fm

Запропонована нова класифікація методів захисту інформації з урахуванням методів перевірки цілісності цифрових сигналів, які на сьогоднішній день викликають найбільший інтерес, проте не мають свого місця в рамках методів та засобів захисту інформації.

Ключові слова класифікація, методи захисту інформації, методи перевірки цілісності, методи активного захисту інформації, методи пасивного захисту інформації

A NEW CLLASSIFICATION OF INFORMATION PROTECTION METHODS

Olena V. Narimanova, Ekaterina A. Trifonova

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: semejka@ua.fm

A new classification of information protection methods including methods of digital signals integrity check is proposed. The last ones today are the most popular but do not have their place among the information protection methods.

Keywords: classification, information protection methods, methods of integrity check, methods of active information protection, methods of passive information protection

УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 2, pp. 169-178

СТЕГАНОГРАФИЧЕСКИЙ МЕТОД ДВУХЭТАПНОГО ДЕКОДИРОВАНИЯ, ОБЕСПЕЧИВАЮЩИЙ АУТЕНТИФИКАЦИЮ КОНТЕЙНЕРА

А.А. Кобозева, М.А. Козина

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: alla_kobozeva@ukr.net

В работе получил дальнейшее развитие стеганографический метод двухэтапного декодирования дополнительной информации, основанный на решении систем линейных алгебраических уравнений, результатом которого стал стеганоалгоритм САБ-SIGN, обеспечивающий одновременное решение двух основных задач стеганографии – скрытой передачи данных и аутентификации контейнера, в качестве которого используется цифровое изображение, с соблюдением надежности восприятия стеганосообщения. Разработанный стеганоалгоритм является устойчивым к возмущающим воздействиям за счет обеспечения малого числа обусловленности задачи декодирования дополнительной информации, является эффективным при выявлении нарушения целостности стеганосообщения. Алгоритм САБ-SIGN является полиномиальным степени два.

Ключевые слова: стеганографический алгоритм, аутентификация, цифровое изображение, число обусловленности, матрица, система линейных уравнений

Введение

Одним из самых важных вопросов, решаемых обществом, на сегодняшний день является обеспечение защиты информации. В настоящий момент общество вступает в период своего развития, который по праву можно назвать информационным. Информация становится одним из основных и самых дорогих товаров [1]. В силу этого большое внимание должно уделяться ее защите, в частности, реализации положений законодательства Украины об авторском праве.

Актуальность проблемы информационной безопасности стимулирует создание новых алгоритмов и методов, позволяющих осуществлять ее защиту. Одно из перспективных направлений защиты информации сформировали современные методы стеганографии [2, 3]. Стеганография представляет собой совокупность методов, основывающихся на различных принципах, которые обеспечивают сокрытие самого факта существования конфиденциальной информации в той или иной среде, а также средств реализации этих методов. А именно, организация скрытого канала связи осуществляется внутри открытого канала: в некоторый контейнер, или основное сообщение (ОС), осуществляется внедрение дополнительной информации (ДИ) так, чтобы результат такого внедрения – стеганосообщение (СС) был зрительно неотличим от ОС [4].

Наибольшая активность на сегодня в научной деятельности в области стеганографии связана с ограничением использования шифрования во многих странах мира, в том числе и в Украине.

Особенность стеганографического подхода позволяет в рамках традиционно существующих информационных потоков или информационной среды решать некоторые важные задачи защиты информации ряда прикладных областей [3,4].

Одним из эффективных решений проблемы защиты авторского права, позволяющих проверить правообладателя цифровых изображений (ЦИ), видео-, звукозаписей, является организация обеспечения аутентичности за счет внедрения цифровых водяных знаков (ЦВЗ) [3]. Разработка методов встраивание ЦВЗ и встраивания ДИ с целью ее скрытой передачи образуют два основных направления развития современной стеганографии, решающих разные задачи. Исходя из важности и актуальности решения этих задач – аутентификации и организации скрытой передачи информации, в открытой печати предлагаются стеганоалгоритмы, осуществляющие их одновременное решение, однако имеющиеся разработки не лишены ряда существенных недостатков [5, 6], оставляя актуальной задачу разработки новых стеганографических алгоритмов, позволяющих одновременно обеспечивать скрытую передачу данных и аутентификацию сигнала-контейнера.

Цель исследования и постановка задания

Эффективность любого стеганографического метода (СМ) определяется рядом характеризующих его работу параметров, среди которых: гарантируемость обеспечения надежности восприятия стеганосообщения; устойчивость СМ к помехам – атакам; величина скрытой пропускной способности [3].

Известно, что на сегодняшний день при организации канала связи очень широко используется метод модификации наименьшего значащего бита (LSB). Однако при его весомых достоинствах, таких как, например, простой реализации, значительной скрытой пропускной способности, он имеет существенный недостаток, немаловажный при передаче СС в канале связи, связанный с чувствительностью СС к любого рода возмущающим воздействиям. В связи с этим в [7] был предложен СМ организации скрытой передачи данных, осуществляющий двухэтапное декодирование ДИ, основанный на решении систем линейных алгебраических уравнений (СЛАУ), позволивший значительно увеличить устойчивость к возмущающим воздействиям существующих стеганоалгоритмов, в частности, LSB, что было обосновано теоретически и проверено при помощи представительных вычислительных экспериментов. Однако разработанный в [7] метод, являясь привлекательным с точки зрения его устойчивости к атакам, не обеспечивает аутентификацию сигнала-контейнера. В связи с этим

Целью работы является модификация СМ двухэтапного декодирования ДИ [7] для обеспечения одновременного решения с его помощью двух основных задач стеганографии – скрытой передачи данных и аутентификации ОС с соблюдением надежности восприятия СС.

Для достижения цели в работе решаются следующие *задачи*:

1) несложной в вычислительном смысле организации пересылки и декодирования ДИ;

2) обеспечения малого числа обусловленности задачи декодирования ДИ;

3) организации обеспечения аутентификации ОС;

4) обеспечения эффективного декодирования ДИ в случае нарушения аутентичности для контейнера, в качестве которого выступает произвольное цифровое изображение.

Основная часть

В качестве ОС рассматривается цветное (модель RGB) ЦИ. СП будет проводится путем возмущения одной из трех матриц, отвечающих контейнеру, например, матрицы красной составляющей (хотя это не принципиально). Обозначим преобразуемую $n \times m$-матрицу контейнера F.

Стеганографическое преобразование изображения будет иметь характер матричных операций [8, 9], и в дальнейшем трактуется как возмущение ОС. Стеганосообщение при пересылке может подвергаться как преднамеренным, так и непреднамеренным атакам, что формализуется в виде дополнительных возмущающих воздействий и может привести к снижению эффективности декодирования ДИ.

Метод пересылки и декодирования ДИ, применяемый в области компьютерной стеганографии, будем называть устойчивым, если формируемое при помощи этого СМ стеганосообщение является нечувствительным (малочувствительным) к возмущающим воздействиям, т.е. декодирование полученной информации производится адресатом с малой результирующей ошибкой при наличии возмущающих воздействий в канале связи.

Разобьем матрицу контейнера F на $s \times s$-блоки (в частности, стандартным разбиением матрицы является разбиение на блоки размера 8×8 [10]). Пусть B — матрица произвольного блока. Далее все преобразования производятся с каждым блоком в отдельности.

В качестве ДИ будем рассматривать сформированный случайным образом бинарный вектор x длины $\left[\frac{n}{s}\right] \times \left[\frac{m}{s}\right]$, где $[\bullet]$ — целая часть аргумента, элементы которого $x_i \in \{-1,1\}$. ДИ может содержать и меньшее количество элементов, тогда она дополняется незначащими элементами до нужной длины.

В каждый блок B встраивается 1 бит ДИ — x_i после его предварительного кодирования, которое осуществляется следующим образом. Биту ДИ x_i ставится в соответствие вектор x^B с элементами $x^B{}_j$ длины s по следующему правилу:

$$x^B{}_j = \begin{cases} 1, \ если \ x_i = 1, \\ -1, \ если \ x_i = -1 \end{cases}, \quad j = \overline{1,s}.$$

Вектор x^B призван обеспечить в дальнейшем проверку аутентичности контейнера, а именно, его части, отвечающей блоку B.

Матрице блока B ставится в соответствие нижняя треугольная матрица $\overline{B}$ с элементами $\bar{b}_{ij}$, $i, j = \overline{1,s}$, в соответствии с соотношением:

$$\bar{b}_{ij} = \begin{cases} 1, если \ i = j, \\ 0, если \ i < j, \\ 1, если \ (i > j) \& (b_{ij} > t) \\ 0, если \ (i > j) \& (b_{ij} \le t) \end{cases}, \quad i, j = \overline{1,s}. \qquad (1)$$

Здесь $t = \dfrac{\max\limits_{i,j} f_{ij} + \min\limits_{i,j} f_{ij}}{2}$, где f_{ij} — элементы матрицы F. Матрица $\overline{B}$ по построению для любого блока B исходной матрицы F ОС нижняя треугольная, невырожденная ($\det \overline{B} = 1$), хорошо обусловленная.

Обозначим v — вектор длины s, отвечающий вектору x^B, получаемый следующим образом:

$$v = \overline{B} x^B. \qquad (2)$$

Вектор v, как следует из (2), будет иметь целые компоненты одного знака. Заметим, что при предположении отсутствия ошибок машинной арифметики, вектор x^B является точным решение системы линейных алгебраических уравнений

$$\overline{B}\, x^B = v. \tag{3}$$

Вектор v погружается в блок B, реализуя тем самым погружение информационного бита x_i ДИ. Для его элементов v_i, $i = \overline{1,s}$, из (2) с учетом вида $\overline{B}$ вытекает:

$$|v_i| \le s, \quad i = \overline{1,s}. \tag{4}$$

В отличии от [11], где аналогичный математический объект подвергается дополнительным преобразованиям для обеспечения надежности восприятия получаемого СС, соотношение (4) позволяет оставить сформированный в соответствии с (2) вектор v без преобразований: мы уходим от выбора дополнительного параметра m, от которого в [11] зависела эффективность декодирования ДИ.

В процессе СП для передачи по каналу связи одного бита x_i ДИ в матрицу B погружается вектор v: в каждый элемент *i*-ой строки блока аддитивно встраивается соответствующее значение v_i, $i = \overline{1,s}$.

При пересылке СС может подвергаться возмущающим воздействиям в канале связи, активным атакующим действиям, что естественным образом изменит его матрицу.

Декодирование ДИ адресатом включает в себя два этапа аналогично [11]. Матрица полученного СС разбивается на $s \times s$-блоки, обозначаемые далее B^S. Из каждого блока B^S на первом этапе декодирования ДИ извлекается в общем случае возмущенный вектор v, обозначаемый v^S, рассматриваемый как правая часть СЛАУ (3), где матрица СЛАУ отвечает нижней треугольной бинарной матрице, построенной для блока B^S аналогично (1), обозначаемая далее $\overline{B}^S$. Выделение информационного вектора $x^B{}_{np}$ с элементами $\left(x^B{}_{np}\right)_i$, $i = \overline{1,s}$, – приближенного для x^B происходит на втором этапе декодирования при решении неоднородной СЛАУ – в общем случае возмущенной системы (3), которая имеет вид:

$$\overline{B}^S x^B{}_{np} = v^S. \tag{5}$$

На этом этапе осуществляется проверка аутентичности ЦИ: в отсутствии возмущающих воздействий на СС при решении СЛАУ (5) для каждого блока матрицы СС

$$\left(x^B{}_{np}\right)_i = 1, \ i = \overline{1,s}, \quad \text{или} \quad \left(x^B{}_{np}\right)_i = -1, \ i = \overline{1,s},$$

что говорит о ненарушенной целостности контейнера. В противном случае СС было подвергнуто возмущающим воздействиям, претерпело несанкционированные изменения.

При выявлении нарушения целостности задача декодирования остается актуальной во многих случаях, в частности, если эти нарушения были непреднамеренными.

Для большинства изображений при малых возмущениях в канале связи $\overline{B}^S \approx \overline{B}$. Отличия этих матриц может быть в тех элементах, которые являются результатом кодирования элементов исходной матрицы из окрестности *t*. Таким образом, с

незначительным допущением в предположении малых возмущений можно считать, что система (5) отличается от системы (3) лишь вектором правой части. В этом случае $x^{B}{}_{пр} \neq x^{B}$. Учитывая вид множества, которому принадлежат элементы x^{B}, заметим, что для осуществления декодирования нас не столько интересуют непосредственные значения элементов $x^{B}{}_{пр}$, сколько их знак. Окончательный шаг декодирования отвечает формуле:

$$\left(\overline{x^{B}}_{пр}\right)_i = sign\left(\left(x^{B}{}_{пр}\right)_i\right), \quad i = \overline{1,s}. \tag{6}$$

Нужно отметить, что при нарушении целостности контейнера элементы вектора $\overline{x^{B}}_{пр}$ могут не оказаться равными. В этом случае предлагается бит ДИ x_i положить равным элементу $\overline{x^{B}}_{пр}$ с наибольшим повторением. Например: если вектор $\overline{x^{B}}_{пр}$ ($s = 8$), полученный в результате операции (6), содержит элементы (-1, -1, 1, 1, -1, -1, -1, -1), то $x_i = -1$.

В случае, когда число включений -1 и 1 в $\overline{x^{B}}_{пр}$ совпадает, то целесообразно брать во внимание знак, соответствующий последнему элементу вектора $\overline{x^{B}}_{пр}$: при получении именно последнего элемента вектора при кодировании, вероятнее всего получить наибольшее возмущение, которое далее не перекроется шумом атакующего, чтобы не привести к видимым нарушениям контейнера.

Вектор $\overline{x^{B}}$ будем называть sign-решением системы (3), а непосредственную реализацию алгоритма, идея которого предложена выше, будем называть САБ-SIGN.

Использование формулы (6) при декодировании, допускает неограниченно большие погрешности при решении (5), которые могут вообще не повлиять на результат декодирования (6), т.е. $\left\|\overline{x^{B}}_{пр} - x^{B}\right\|$ может быть сколь угодно велика, если при этом выполняются условия: $sign\left(x^{B}{}_i\right) = sign\left(\left(\overline{x^{B}}_{пр}\right)_i\right)$, $i = \overline{1,s}$. Таким образом, даже очень большие возмущения правой части системы при формировании v, о которых говорилось выше, сохраняющие знаки элементов вектора, могут не отразиться на результате декодирования.

Предложенный подход к решению СЛАУ дает возможность при декодировании получить ответ о нарушении/сохранении целостности контейнера, а также, как показывают результаты вычислительного эксперимента, получить большой объем правильно восстановленной информации даже при больших возмущениях входных данных.

Результаты вычислительного эксперимента.

Целью вычислительного эксперимента является практическая проверка эффективности разработанного стеганографического метода.

Одним из показателей, используемых для оценки эффективности метода является объем правильно восстановленной ДИ при одинаковых условиях проведения эксперимента, который вычисляется по формуле:

$$P = \frac{\text{Кол – во бит секретного сообщения, восстановленных верно}}{\text{Общее кол – во бит секретного сообщения}} \times 100\% \tag{1}$$

Все вычислительные эксперименты проводились в среде *MathWorks* MATLAB на 200 изображениях, сохраненных после СП, проводимого САБ-SIGN, в формате без

потерь. Возмущающие воздействия на СС моделировались путем наложения в пространственной области различных шумов с различными параметрами (табл. 1). Нарушение целостности СС в проведенном эксперименте было зафиксировано в 100% случаев, что говорит об эффективности использования САБ-SIGN с целью аутентификации ОС.

Таблица 1.

Зависимость объема правильно декодированной информации P от уровня шума, наложенного на стеганосообщение

Шум	Среднеквадратичное отклонение σ	P (%), при наложении шума	
		на все изображение	на красную составляющую изображения
Гауссовский	0.01	68	62
	0.001	82	71
	0.0001	96	94
	0.00001	99.9	98
Мультипликативный	0.01	87	87
	0.001	95	96
	0.0001	98	98
	0.00001	99.9	99
Пуассоновский		90	89

Процесс СП методом САБ-SIGN не нарушает надежность восприятия полученного СС, в отличие от процесса наложения аддитивного гауссовского шума со среднеквадратичным отклонением более 0.0001 (рис. 1), который, однако, сохраняет высокую эффективность декодирования ДИ (табл. 1). Результаты определялись как среднее арифметическое для 200 тестируемых ЦИ для каждого параметра шума.

Рассмотрим подробно вопрос выбора размера блока B. Из (4) следует, что наибольшие по модулю значения элементов вектора v, равны s. Уменьшение/увеличение размера блока приведет к уменьшению/увеличению возмущения пикселей ЦИ-контейнера в процессе СП. Чем больше размер блока, на который разбивается матрица ОС, тем больше эта матрица получит возмущение в процессе погружения ДИ, что, во-первых, приведет к уменьшению чувствительности СС к возмущающим воздействиям, что является положительным фактором (см. рис. 3, 4), но, во-вторых, может привести к нарушению надежности восприятия СС, а в-третьих, уменьшит скрытую пропускную способность организуемого стеганографического канала связи.

Заметим, что не целесообразно использовать блоки, для которых $s < 4$. Действительно, в этом случае, с учетом (4), СП приведет к незначительным возмущениям матрицы ОС, результатом чего станет СС, чувствительное к любым возмущающим воздействиям.

Как следует из результатов вычислительного эксперимента (рис. 3, 4), наиболее предпочтительным с точки зрения устойчивости является САБ-SIGN, использующий блоки размера 16×16. Однако использование таких блоков может привести к нарушению надежности восприятия СС, а также уменьшает в четыре (шестнадцать) раза скрытую пропускную способность организуемого канала связи, по сравнению с 8×8- (4×4-) блоками. В тоже время объем P верно декодированной информации в случае 16×16-блоков незначительно отличается от значения P при выборе блока размером 8×8. Таким образом, для САБ-SIGN рекомендуется использовать блоки стандартного разбиения - 8×8.

а

б

в

г

д

Рис. 1. Изображение Image и его преобразования путем внедрения ДИ и наложения аддитивного гауссовского шума с нулевым матожидаем и различными значениями среднеквадратичного отклонения σ: а – исходное ЦИ; б – СС; в – $\sigma = 0.01$; г – $\sigma = 0.001$; д – $\sigma = 0.0001$

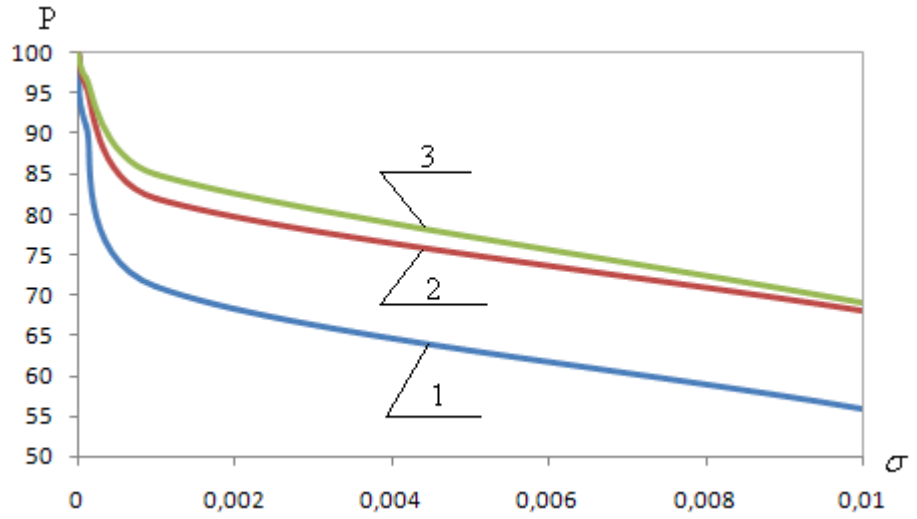


Рис. 3. Зависимость объема декодированной информации от параметра накладываемого на СС аддитивного гауссовского шума при различных размерах блока матрицы: 1 – $s=4$; 2 – $s=8$; 3 – $s=16$

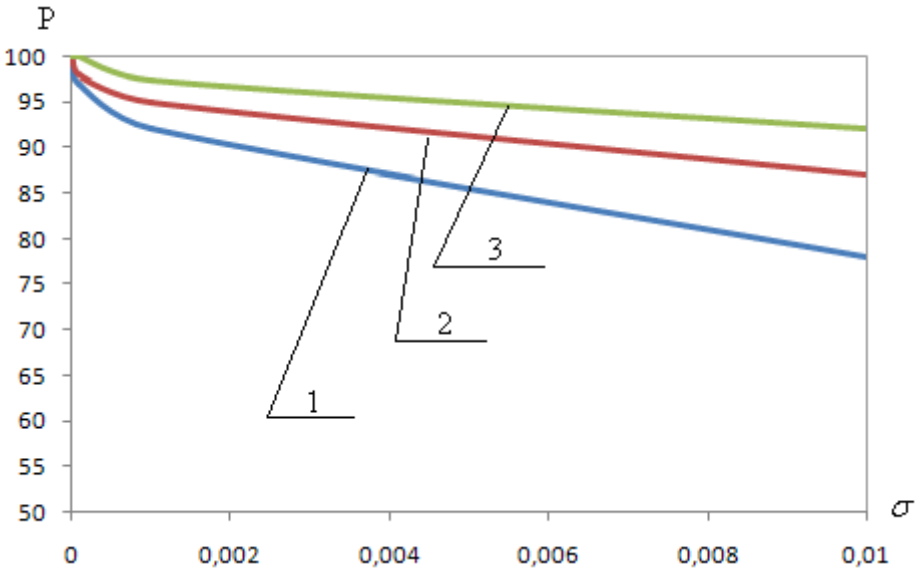


Рис. 4. Зависимость объема декодированной информации от параметра накладываемого на СС мультипликативного шума при различных размерах блока матрицы: 1 – $s=4$; 2 – $s=8$; 3 – $s=16$

Заключение

В работе предложена модификация СМ двухэтапного декодирования ДИ, основанного на решении СЛАУ, обеспечивающая одновременное решение двух основных задач стеганографии – скрытой передачи данных и аутентификации контейнера с соблюдением надежности восприятия СС.

Разработанный стеганоалгоритм САБ-SIGN является устойчивым к возмущающим воздействиям за счет обеспечения малого числа обусловленности задачи декодирования ДИ. Объем восстановленной ДИ в условиях наложения шума составил $P > 90\%$ при $\sigma < 0.001$ для аддитивного гауссовского и мультипликативного шумов, что говорит о высокой эффективности САБ-SIGN.

При нарушении целостности СС, сформированного САБ-SIGN, это нарушение было выявлено в 100% случаев.

Вычислительная сложность разработанного алгоритма определяется как $\underline{O}\left(n^2\right)$ для $n \times n$-матрицы контейнера.

Все вышесказанное позволяет утверждать, что цель работы достигнута.

Список литературы

1. Хорошко, В.А. Методы и средства защиты информации [Текст] : научное издание / В.А. Хорошко, А.А. Чекатков; Ред. Ю.С. Ковтанюк. — К. : ЮНИОР, 2003. — 505 с.
2. Кобозєва, А.А. Аналіз захищеності інформаційних систем / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко. — К. : Вид. ДУІКТ, 2010. — 316 с.
3. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
4. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
5. Глумов, Н.И. Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации / Н.И. Глумов, В.А. Митекин // Компьютерная оптика. — 2011. — Том 35, № 2. — С. 262–267.
6. Кобозева, А.А. Стеганографический алгоритм скрытой передачи информации, обеспечивающий аутентификацию контейнера / А.А. Кобозева, А.Д. Шовкун // Науковий вісник Міжнародного гуманітарного університету. Серія: Інформаційні технології та управління проектами. — 2012. — № 4. — С. 21–28.
7. Кобозева, А.А. Стеганографический метод, основанный на решении систем линейных алгебраических уравнений / А.А. Кобозева, А.В. Коломийчук // Праці УНДІРТ. — 2006. — № 1(45)–2(46). — С. 104–108.
8. Деммель, Д. Вычислительная линейная алгебра [Текст] : теория и приложения / Д. Деммель; Пер. с англ. Х.Д. Икрамова. — М. : Мир, 2001. — 430 с.
9. Гантмахер, Ф.Р. Теория матриц [Текст] : монография / Ф.Р. Гантмахер. — 5-е изд. — М. : Физматлит, 2004. — 559 с.
10. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М. : Техносфера, 2006. — 1070 с.
11. Кобозева, А.А. Практическая реализация стеганографического метода, основанного на решении системы линейных алгебраических уравнений / А.А. Кобозева, И.И. Борисенко // Праці УНДІРТ. — 2006. — № 3(47). — С. 78–83.

СТЕГАНОГРАФІЧНИЙ МЕТОД ДВОЕТАПНОГО ДЕКОДУВАННЯ, ЩО ЗАБЕЗПЕЧУЄ АУТЕНТИФІКАЦІЮ КОНТЕЙНЕРА

А.А. Кобозєва, М.О. Козіна

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: alla_kobozeva@ukr.net

У роботі отримав подальший розвиток стеганографічний метод двоетапного декодування додаткової інформації, заснований на рішенні систем лінійних алгебраїчних рівнянь, результатом якого став стеганоалгоритм САБ-SIGN, що забезпечує одночасне рішення двох основних задач стеганографії – прихованої передачі даних і автентифікації контейнера, у якості якого використовується цифрове зображення, з дотриманням надійності сприйняття стеганоповідомлення. Розроблений стеганоалгоритм є стійким до збурних дій за рахунок забезпечення малого числа обумовленості задачі декодування додаткової інформації, є ефективним при виявленні порушення цілісності стеганоповідомлення. Алгоритм САБ-SIGN є поліноміальним ступеня два.

Ключові слова: стеганографічний алгоритм, автентифікація, цифрове зображення, число обумовленості, матриця, система лінійних рівнянь

THE STEGANOGRAPHIC METHOD WITH A TWO-STAGE DECODING WHICH PROVIDS AUTHENTIFICATION THE CONTAINER

Alla A. Kobozeva, Mariya A. Kozina

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: alla_kobozeva@ukr.net

The steganographic method with a two-stage decoding of additional information, based on the decision of the systems of linear algebraic equalizations, the result of which has become steganoalgorithm SAB-SIGN, providing at the same time the decision for two basic tasks of steganography – the hidden data of communication and authentification the container as digital image, with the observance of reliability perception of steganomessage, has got further development in this article. Steganoalgorithm which was developed is steady to revolting influences due to providing a small number of conditionality of the task with decoding the additional information, is effective at the exposure of violation integrity of the steganomessage. An algorithm of SAB-SIGN is polynomial with second degree.

Keywords: steganographic algorithm, authentication, digital image, number of conditionality, matrix, system of linear equalizations

УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 2, pp. 179-189

СТЕГАНОАНАЛИЗ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ, ХРАНЯЩИХСЯ В ПРОИЗВОЛЬНЫХ ФОРМАТАХ

И.А. Узун

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: uzun.illya@gmail.com

Работа посвящена разработке стеганоаналитического алгоритма выявления наличия секретного сообщения, погруженного в цифровое изображение методом модификации наименьшего значащего бита. Алгоритм основан на анализе пар цветов, применим для контейнера-изображения, хранимого в произвольном формате.

Ключевые слова: стеганография, стеганоанализ, близкие пары цветов, уникальные цвета, сокрытие информации

Введение

Компьютеризация и информатизация, всевозрастающая роль знаний и технологий приводят к становлению информационного общества. Одними из характерных черт такого общества является активное использование цифровых технологий, развитие информационной экономики, электронного государства и электронных социальных сетей. Важная роль в информационном обществе возложена на информационное пространство. Информационное пространство должно обеспечивать эффективное информационное взаимодействие людей, их доступ к мировым информационным ресурсам, удовлетворять потребности людей в информационных продуктах и услугах. Большую значимость в информационном пространстве приобретает проблема обеспечения конфиденциальности и конфиденциальной информации. Данную проблему, проблему предотвращения разглашения какой-либо информации, способна решить как криптография, так и стеганография [1, 2].

Целью криптографии является модификация секретного конфиденциального сообщения, чтобы его в зашифрованном виде было невозможно прочесть перехватчику. При этом криптография не заботится о том, что зашифрованное сообщение может привлекать к себе внимание. Стеганография же, в отличие от криптографии, скрывает передаваемую информацию внутри контейнера или основного сообщения (ОС), который сам по себе не вызывает никаких подозрений и, соответственно, в тайне остается сам факт передачи. Таким образом, преимущество стеганографических методов и алгоритмов состоит в том, что они предоставляют возможность скрытно передать дополнительную информацию (ДИ) – конфиденциальное сообщение, одновременно с ОС – открытой информацией. В качестве ОС может быть выбран любой мультимедиа объект – цифровое изображение (ЦИ), видео или аудио (в настоящей работе как контейнер используется ЦИ). В результате погружения ДИ в ОС не должно происходить заметных изменений контейнера. Данный процесс будем называть стеганопреобразованием (СП), а его результат – стеганосообщением (СС).

Использование СП часто позволяет избежать прямых атак на ДИ, поскольку неизвестно, присутствует ли она в информационном потоке. ДИ, вносимая в контейнер, может быть предварительно зашифрована, чтобы усложнить основную задачу

стегоанализа (СА) [1, 2] – установление факта присутствия в контейнере скрытой информации.

Большое количество программных средств (*Steganos*, *StegHide*, *S-tools* и др.) как платных, так и бесплатных, свободно распространяемых через Интернет, сделали стеганографию очень популярным средством для сокрытия информации. Совсем недавно Эдвардом Сноуденом была разглашена закрытая секретная информация [3, 4] о существовании программ компьютерного слежения PRISM (США) и Tempora (Великобритания), прослушивающих телефонные разговоры и Интернет-трафик в максимально возможных объемах. PRISM позволяет просматривать электронную почту (Microsoft Hotmail, Google Mail, Yahoo), прослушивать голосовые и видео-чаты, просматривать фотографии, видео, отслеживать пересылаемые файлы и узнавать любые другие подробности из социальных сетей (Facebook, YouTube, Skype). Очевидно, что в свете подобных обстоятельств, к использованию стеганографии прибегнет еще большее число людей, использующих упомянутые сервисы электронной почты и социальные сети, чтобы сохранить конфиденциальность своей информации, не привлекая при этом внимания, как если бы это были зашифрованные файлы.

Известно, что посредством стеганографии между собой общаются как секретные государственные службы, шпионы [5], так и криминальные структуры, и террористы [6–8]. (Упомянутые выше программы PRISM, Tempora как раз и были созданы для борьбы с терроризмом, хоть и нарушая при этом права и свободы честных людей.) Стеганография также может быть использована как способ организации утечки ценной информации из компаний и т.д. Поэтому развитие методов СА на сегодняшний день является чрезвычайно *актуальной* задачей.

СА осуществляет поиск и анализ определенных характеристик и признаков в исследуемом цифровом объекте, установление факта наличия или отсутствия которых позволяет получить ответ на вопрос, является ли анализируемый объект СС или же он не подвергался СП.

Как говорилось ранее, уже создано достаточное количество стеганографических средств, применяемых для различных цифровых контейнеров. Большинство таких продуктов применяет различные модификации LSB-метода, или метода модификации наименьшего значащего бита, основной идеей которого является использование одного или нескольких младших двоичных разрядов интенсивности цветовых компонент отдельных пикселей для внедрения ДИ. Популярность данного метода обусловлена его простотой и тем, что он позволяет скрывать в относительно небольших файлах достаточно большие объемы информации [9]. Визуально изображение при этом не изменяется, особенно если в качестве ОС выбрано многоцветное изображение с большим количеством деталей, то есть информационно нагруженное. Если, например, взять ЦИ цветовой модели RGB, на каждую компоненту цвета R, G и B которого отводится 8 бит, и изменить значения наименьших значащих бит (НЗБ) – то подобное искажение будет неуловимо для человеческого восприятия [10]. Это в значительной степени осложняет работу стегоаналитика, если он не обладает специальными средствами СА. В качестве таких средств могут выступать программы, реализующие методы и алгоритмы стегоанализа.

Хорошо зарекомендовали себя при выявлении LSB-метода стеганоаналитические алгоритмы, основанные на анализе пар цветов [11–15]. Однако, они не лишены существенных недостатков, что осложняет их использование. Так существующие алгоритмы нацелены на работу с конкретными форматами хранения анализируемых изображений. При этом алгоритмы, работающие с форматами без потерь, прибегают к дополнительной категоризации ЦИ [11, 13] с последующим определением пороговых значений для каждой категории. Однако предложенная классификация является неполной и неубедительной, базируется на субъективном мнении исследователей. Для алгоритмов, работающих с ЦИ, хранимыми в форматах с потерями [14], существует

ограничение относительно количества уникальных цветов в ЦИ. Область их применимости – ЦИ, количество уникальных пикселей в которых не превышает половину общего числа пикселей. Данное условие значительно сужает область применимости предлагаемых стеганоаналитических алгоритмов даже для сжатых с потерями изображений.

В силу вышесказанного, создание нового стеганоаналитического метода выявления наличия секретной информации, погруженной при помощи LSB-метода, основанного на анализе пар цветов цифрового изображения, свободного от перечисленных выше недостатков, не зависящего от формата хранения анализируемого ЦИ, является *актуальной* задачей.

Цель и постановка исследований

Целью статьи является разработка стеганоаналитического алгоритма (САА), основанного на анализе количества близких пар цветов и уникальных цветов, применимого для ЦИ, хранимых в произвольном формате (с потерями, без потерь).

Для достижения поставленной цели необходимо решить следующие *задачи*:

1) Определить статистические характеристики ОС и СС, анализ которых, позволит отделить ЦИ, подвергавшиеся СП, от ЦИ, не содержащих ДИ;

2) Выявить характерные особенности и отличия ЦИ, не подвергавшихся СП, от СС, полученных после внедрения ДИ в ходе СП посредством модификации НЗБ;

3) Выявить характерные особенности и отличия изображений, уже подвергавшихся СП посредством модификации НЗБ, от СС, полученных после повторного СП;

4) Исходя из результатов решения предыдущих задач, разработать САА для выявления СС, полученных путем использования метода LSB;

5) Провести анализ эффективности разработанного САА;

6) На основании результатов, полученных при анализе эффективности разработанного САА, определить пороговое значение используемого алгоритмом параметра, при котором ошибки первого и второго рода будут минимальными.

Основная часть

Введем необходимые обозначения и определения. Под цветом в дальнейшем будем понимать тройку компонент (R,G,B) или пиксель, который также подразумевается как триплет значений (R,G,B), где R — красная, G — зеленая и B — синяя компонента в цветовой модели RGB [10].

В качестве статистических характеристик для анализа выбраны коэффициенты близких пар цветов и уникальных цветов.

Пусть P — число близких пар цветов в изображении. Согласно определению, данному в [12] (для ЦИ, хранимых в форматах без потерь), под близкой парой понимают два цвета (R_1,G_1,B_1) и (R_2,G_2,B_2), если для них справедливо следующее соотношение:

$$\begin{cases} |R_1-R_2|\le 1, \\ |G_1-G_2|\le 1, \\ |B_1-B_2|\le 1 \end{cases} \Leftrightarrow \quad (R_1-R_2)^2+(G_1-G_2)^2+(B_1-B_2)^2\le 3. \qquad (1)$$

Для изображений, хранимых в формате с потерями, в [16] было введено следующее определение для соотношения цветов близкой пары:

$$\begin{cases} |R_1 - R_2| \le 2, \\ |G_1 - G_2| \le 2, \\ |B_1 - B_2| \le 2 \end{cases} \Leftrightarrow \quad (R_1 - R_2)^2 + (G_1 - G_2)^2 + (B_1 - B_2)^2 \le 12. \qquad (2)$$

Выбор того, что разность соответствующих цветовых компонент двух пикселей не должна превышать по модулю 2 в соотношении (2) было обусловлено тем, что в процессе сохранения ЦИ в JPEG (с потерями) происходит обнуление высокочастотных (и, возможно, некоторых среднечастотных) коэффициентов дискретного косинусного преобразования (ДКП) 8×8-блоков, полученных после стандартного разбиения матрицы исходного изображения. Исключение высоких (и, возможно, средних) частот в JPEG ЦИ никак не восполнится при его пересохранении в формате TIF, поэтому матрица изображения, сохраненного в TIF первоначально и сохраненного в TIF после JPEG-сжатия должны качественно отличаться друг от друга по своим характеристикам [17]. Таким образом, соотношение (1), как проверено в ходе представительного вычислительного эксперимента, является «нерабочим» для контейнеров с потерями, поскольку в результате квантования частотных коэффициентов ЦИ, происходящего в процессе сжатия, количество цветов снижается. Именно эта принципиальная проблема не позволяла до сих пор использовать САА, основанный на анализе пар цветов для ОС с потерями [11, 13, 15].

Согласно определению уникального цвета в [11, 13] для ЦИ в форматах без потерь, два цвета (R_1, G_1, B_1) и (R_2, G_2, B_2) будем называть уникальными, если выполняется, хотя бы одно из условий:

$$\begin{aligned} |R_1 - R_2| &\le 1, \\ |G_1 - G_2| &\le 1, \\ |B_1 - B_2| &\le 1. \end{aligned}$$

Согласно причине изложенной выше, по которой было введено соотношение (2), в [16] было введено определение уникальных цветов в ЦИ, хранимых в формате с потерями. Так, два цвета (R_1, G_1, B_1) и (R_2, G_2, B_2) называются уникальными, если выполняется, хотя бы одно из условий:

$$\begin{aligned} |R_1 - R_2| &\le 2, \\ |G_1 - G_2| &\le 2, \\ |B_1 - B_2| &\le 2. \end{aligned} \qquad (3)$$

Пусть R — отношение количества близких пар цветов P к количеству уникальных цветов U, определяемых согласно (2), (3) соответственно:

$$R = \frac{P}{U}. \qquad (4)$$

Коэффициент R играет ключевую роль при отделении ОС от СС в разработанном САА. Как уже говорилось ранее, процесс стеганоанализа в предлагаемом алгоритме включает в себя операции внедрения ДИ в анализируемый контейнер. Было замечено,

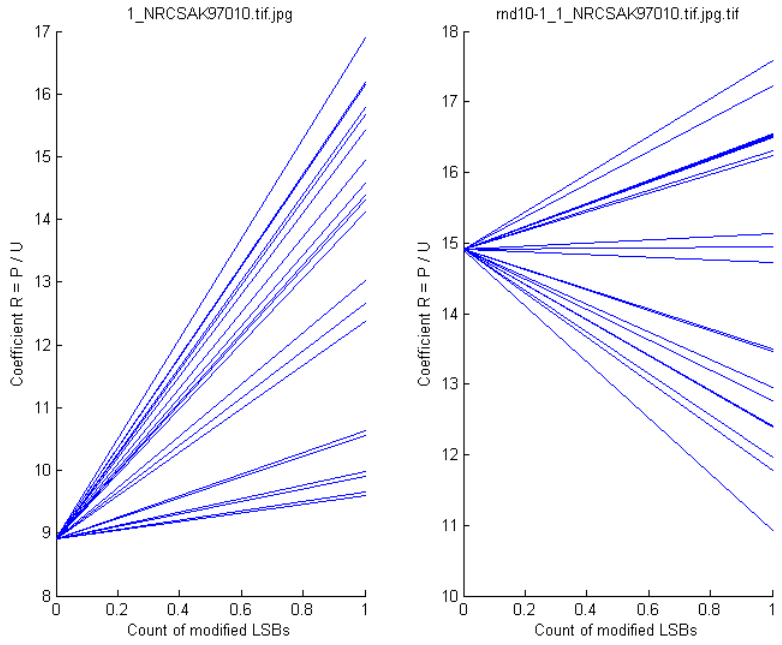
что для точности детектирования целесообразно выполнять не одно, а n СП, которые отличаются лишь внедряемой ДИ.

В [18] был предложен общий математический подход к анализу состояния и технологии функционирования информационных систем, в частности – систем защиты информации. Данный подход основан на теории возмущений и матричном анализе. Процесс получения СС при внедрении ДИ в контейнер посредством LSB-метода, согласно [18], можно представить, как результат воздействия на матрицу контейнера F матрицей возмущения ΔF:

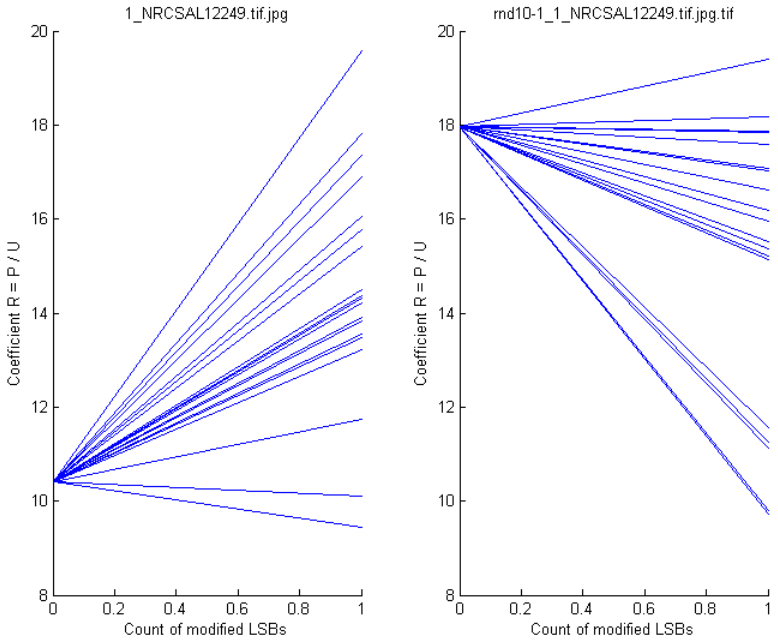
$$\overline{F} = F + \Delta F,$$

где $\overline{F}$ — матрица СС, ΔF — матрица возмущения или ДИ, и F — матрица ОС. Матрица возмущения ΔF, исходя из смысла метода модификации НЗБ, содержит лишь элементы из множества $\{-1,0,1\}$. Для того, чтобы произвести n СП над F, случайным образом осуществляется генерирование n матриц ΔF. Говоря об объеме погружаемой ДИ в процентах, следует понимать, что именно такой процент ненулевых элементов будет содержать матрица ΔF. В основу предлагаемого САА, выполняющего детектирование СС и ОС, было принято положить анализ коэффициентов R и R' из (4). Коэффициент R определяется для матрицы F, а значения R' — для каждой из n матриц ΔF. При работе с ЦИ, хранящимися в формате с потерями, используется соотношение (2), а для ЦИ, не подвергавшихся сжатию, соответственно — (1). На основании сравнения показателей R и R', с использованием при этом порогового значения, делается вывод о наличии либо отсутствии ДИ в анализируемом ЦИ.

На рис. 1, как на примере анализа двух разных изображений, хранимых изначально в формате с потерями, показано, как изменяется отношение близких пар цветов к уникальным цветам (коэффициент R, R') при проведении СП над контейнерами (рис. 1(а)), не содержащими ДИ изначально, и над СС (рис. 1(б)). Ось ординат – значения R и R', ось абсцисс – это количество изменяемых НЗБ. Каждый из графиков состоит из n отрезков. Ордината точки, из которой исходят отрезки – соответствует коэффициенту R, конечные точки отрезков – это n коэффициентов R'.



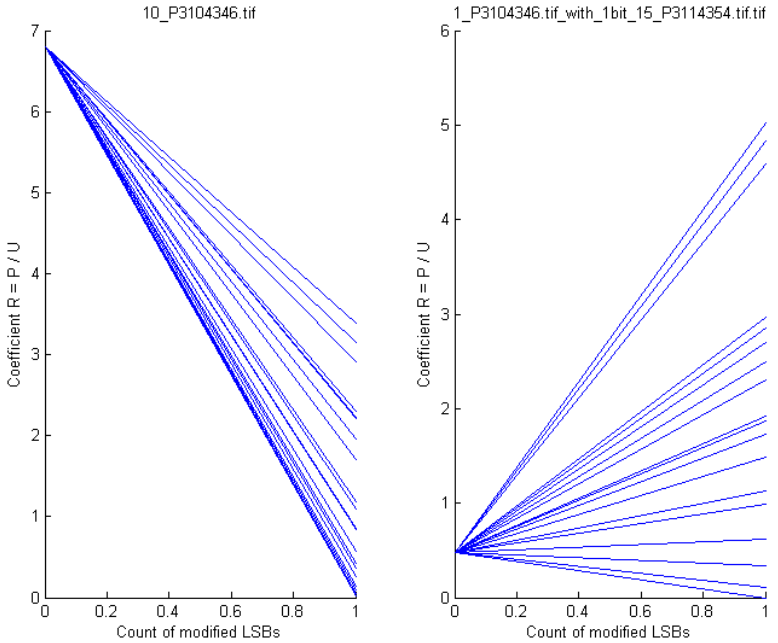
а



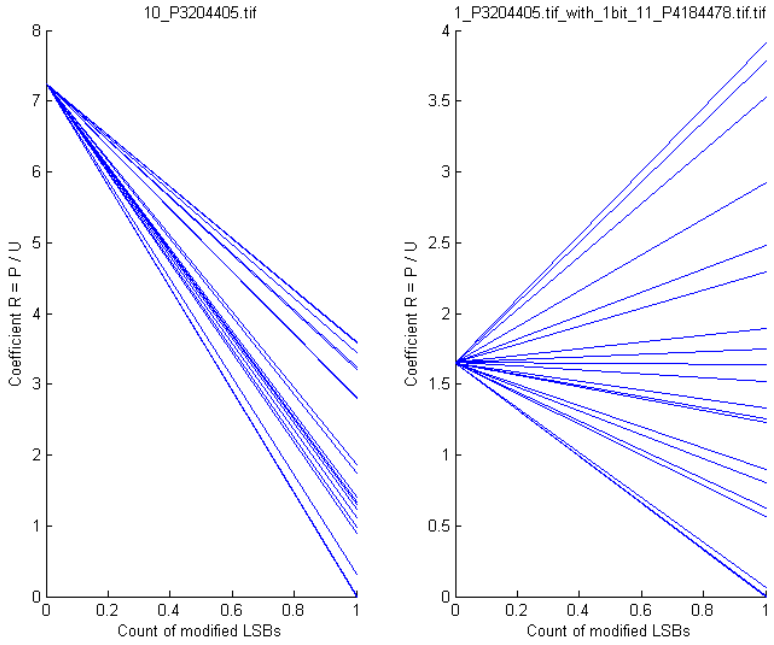
б

Рис. 1. Графики изменения коэффициентов R и R' при СП хранимых в формате JPEG: а – в ЦИ, не содержащих ДИ; б – в СС

Аналогичные графики для изображений, хранившихся изначально в формате без потерь, представлены на рис. 2:



а



б

Рис. 2. Графики изменения коэффициентов R и R' при СП хранимых в формате TIFF: а – в ЦИ, не содержащих ДИ; б – в СС

Как видно из рисунков 1 и 2, характер изменения отношений близких пар цветов к уникальным цветам значительно отличается в зависимости от того, в каком формате изначально хранилось ЦИ. В первую очередь данная особенность объясняется в силу выкладок, изложенных для введения соотношения (2).

Однако данный факт не мешает ввести различные условия для анализируемых контейнеров, в зависимости от того, в каком формате (с потерями или без потерь) изначально хранилось ЦИ.

Для детектирования СС и ОС в ЦИ, хранившихся в формате с потерями, в качестве оцениваемого значения предложена величина $(R - \min(R'))$, а для ЦИ, хранившихся в формате без потерь $(R - \max(R'))$.

Обозначим через T_1, T_2 — величины пороговых значений, минимизирующих ошибки первого и второго рода, для изображений хранимых с потерями и без потерь соответственно.

Тогда, для ЦИ, хранившихся в JPEG (в формате с потерями), будем считать, что матрица F не подвергалась возмущению ΔF, если выполняется условие:

$$R - \min(R') < T_1,$$

иначе считаем анализируемый контейнер СС.

Для ЦИ, хранившихся в TIFF (в формате без потерь), будем считать, что матрица F не подвергалась возмущению ΔF, если выполняется условие:

$$R - \max(R') > T_2,$$

иначе считаем анализируемый контейнер СС.

Предложенный алгоритм был протестирован на выборке из 300 ЦИ, хранимых в формате JPEG, размером 500×500 пикселей, загруженных из базы изображений NRCS [19]. В ходе экспериментов, отдельно анализировались контейнеры, а также СС. Для

оценки эффективности САА были получены специально выборки из СС, в которых были модифицированы все 3 цветовых канала, отдельно только два канала и только один канал. При этом для каждого из этих вариантов были также получены наборы СС в зависимости от объема внедренной ДИ, который был выбран на уровне 20, 35 и 50%. В результате данного анализа была определена оптимальная величина T_1, значение которой составило $T_1 = 1.23$. Ошибки первого и второго рода составили порядка 0.5%. Данные результаты проиллюстрированы на рис. 3:

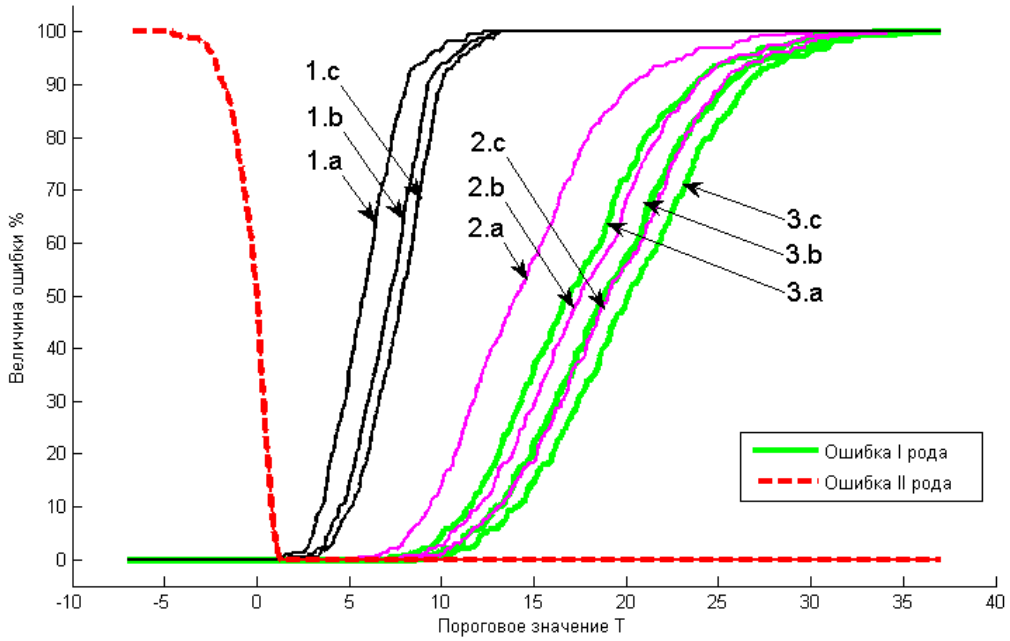


Рис. 3. График зависимости ошибок I и II рода от выбора порогового значения в ЦИ, хранившихся в формате с потерями: 1.a, 1.b, 1.c – в СС изменялся один цветовой канал с объемом ДИ 20, 35 и 50% соответственно; 2.a, 2.b, 2.c – в СС изменялось два цветовых канала с объемом ДИ 20, 35 и 50% соответственно; 3.a, 3.b, 3.c – в СС изменялось три цветовых канала с объемом ДИ 20, 35 и 50% соответственно

Ось ординат на рис. 3 – это величина ошибок первого, либо второго рода. Ось абсцисс – это значение выбираемого порогового значения T_1. Пунктиром изображен график зависимости ошибки второго рода от T_1. Сплошными изображены графики зависимости ошибки первого рода, соответствующие разным наборам СС относительно объема внедренной ДИ. Самый левый график, таким образом, соответствует набору СС, в которые был внедрен наибольший объем ДИ.

Для тестирования САА на изображениях, хранимых в формате без потерь, была использована собственная база из 100 TIFF изображений размером 500×500 пикселей. Была создана выборка из контейнеров, а также выборка из СС, полученных путем замены НЗБ ОС битовой плоскостью случайного ЦИ. Объем внедренной ДИ при этом мог составить порядка 1 бита на пиксель в худшем случае. В результате данного эксперимента величина порогового значения была определена на уровне $T_2 = 0.28$, а ошибка первого и второго рода составила 1% (рис. 4).

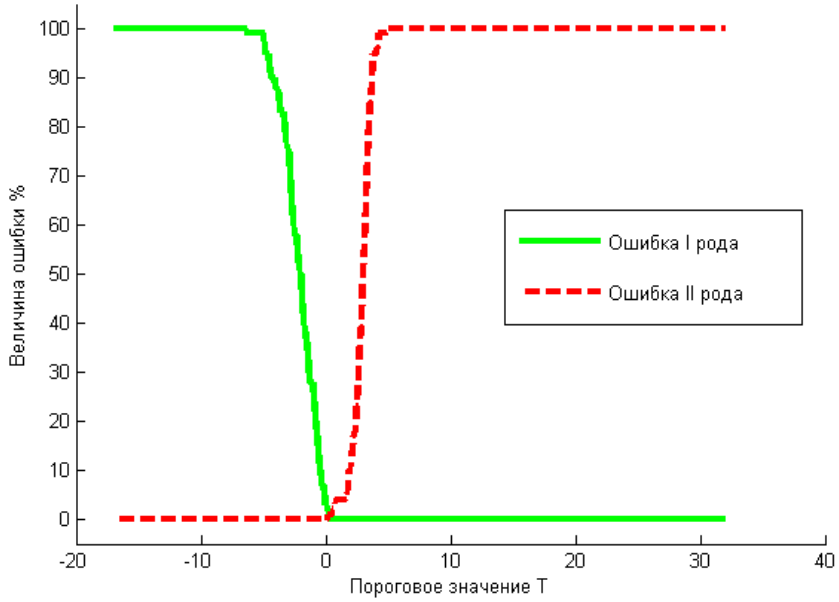


Рис. 4. График зависимости ошибок I и II рода от выбора порогового значения в ЦИ, хранившихся в формате без потерь

Заключение

Результаты вычислительного эксперимента, проведенного с целью проверки эффективности работы нового САА, представлены в таблице 1.

Таблица 1.

Результаты работы предложенного САА

	Порог	Ошибки I рода, %	Ошибки II рода, %	Объем внедренной информации, бит/пиксель
ОС формата с потерями	$T_1 = 1.23$	0.5	0.5	0.2
ОС формата без потерь	$T_2 = 0.28$	1	1	1

В настоящий момент основные усилия автора направлены на увеличение эффективности САА при уменьшении объема внедряемой ДИ для контейнеров, хранимых в формате без потерь.

Список литературы

1. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
2. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
3. O'Harrow Jr, R. U.S., company officials: Internet surveillance does not indiscriminately mine data *[Электронный ресурс]* / R. O'Harrow Jr., E. Nakashima and B. Gellman // The Washington Post.

Washington, USA. Режим доступа: http://articles.washingtonpost.com/2013-06-08/world/39834622_1_prism-clapper-jr-fisa-court (Дата обращения: 08.06.2013).
4. Greenwald, G. NSA Prism program taps in to user data of Apple, Google and others *[Электронный ресурс]* / G. Greenwald, E. MacAskill // The Guardian. London, UK. Режим доступа: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (Дата обращения: 26.05.2013).
5. Fox, S. FBI: Russian Spies Hid Codes in Online Photos *[Электронный ресурс]* // NBC News. New York, USA. Режим доступа: http://www.nbcnews.com/id/38028696/ns/technology_and_science-science/t/fbi-russian-spies-hid-codes-online-photos/ (Дата обращения: 26.05.2013).
6. Бобок, И.И. Стеганоанализ, как частный случай анализа информационной системы / И.И. Бобок, А.А. Кобозева // Сучасна спеціальна техніка. — 2011. — № 2. — С. 21–34.
7. Gul, G. SVD-Based Universal Spatial Domain Image Steganalysis / G. Gul, F. Kurugollu // IEEE Transactions on Information Forensics and Security. — 2010. — Vol. 5, No. 2. — PP. 349–353.
8. Kelley, J. Terrorist instructions hidden online *[Электронный ресурс]* // USA Today. Tysons Corner, Virginia, USA. Режим доступа: http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen-side.htm (Дата обращения: 26.05.2013).
9. Швидченко, И.В. Анализ криптостеганографических алгоритмов / И.В. Швидченко // Проблемы управления и информатики. — 2007. — № 4. — С. 149–155.
10. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М. : Техносфера, 2006. — 1070 с.
11. Geetha, S. Close color pair signature ensemble adaptive threshold based steganalysis for LSB embedding in digital images / S. Geetha, S. Sindhu, and N. Kamaraj // Transactions on Data Privacy. — 2008. — Vol. 1, Iss. 3. — PP. 140–161.
12. Johnson, N.F. Exploring Steganography: Seeing the Unseen / N.F. Johnson, S.Jajodia // IEEE Computer. — 1998. — Vol. 31, No. 2. — PP. 26−34.
13. Mitra, S. Steganalysis of LSB Encoding in Uncompressed Images by Close Color Pair Analysis / S. Mitra, T. Roy, D. Mazumdar and A.B. Saha // IIT Kanpur Hackers' Workshop 2004 (IITKHACK04), 23–24 Feb 2004. — 2004. — PP. 23–24.
14. Fridrich, J. Steganalysis of LSB Encoding in Color Image / J. Fridrich, R. Du, M. Long // IEEE International Conference on Multimedia and Expo. — 2000. — Vol.3. — PP. 1279–1282.
15. Seymer, P. Performance Optimization of Close-Color Pair Steganalysis / P. Seymer, G. Dimitoglou // Proceedings of the 2007 International Conference on Security & Management, Las Vegas, USA. — 2007. — PP. 123–127.
16. Рудницкий, В.Н. Стеганоаналитический алгоритм для изображений, подвергавшихся операции сжатия с потерями / В.Н. Рудницкий, И.А. Узун // Захист інформації. — 2013. — Том 15, № 2. — С. 122–127.
17. Бобок, И.И. Стеганоаналитический алгоритм для основного сообщения, хранимого в форматах с потерями / И.И. Бобок // Вісник Національного технічного університету «ХПІ». — 2012. — №29. — С. 41–49.
18. Кобозєва, А.А. Аналіз захищеності інформаційних систем [Текст] : підруч. для студ. вищ. навч. закл., які навч. за напр. «Інформаційна безпека» та «Системні науки та кібернетика» / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко ; М-во трансп. та зв'язку України, Держ. ун-т інформ.-комунікац. технологій. — К. : ДУІКТ, 2010. — 316 с.
19. NRCS Photo Gallery: *[Электронный ресурс]* // United States Department of Agriculture. Washington, USA. Режим доступа: http://photogallery.nrcs.usda.gov (Дата обращения: 26.07.2012).

СТЕГАНОАНАЛІЗ ЦИФРОВИХ ЗОБРАЖЕНЬ, ЩО ЗБЕРІГАЮТЬСЯ У ДОВІЛЬНИХ ФОРМАТАХ

І.А. Узун

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; email: uzun.illya@gmail.com

Робота присвячена розробці стеганоаналітичного алгоритму визначення наявності секретного повідомлення, вбудованого в цифрове зображення. Запропонований алгоритм не залежить від формату зберігання зображення. Алгоритм заснований на аналізі пар кольорів з використанням методу модифікації найменшого значущого біту.

Ключові слова: стеганографія, стеганоаналіз, близькі пари кольорів, унікальні пари кольорів, приховування інформації

STEGANALYSIS OF DIGITAL IMAGES THAT SAVED IN RANDOM FILE FORMATS

Illya A. Uzun

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; email: uzun.illya@gmail.com

This paper is devoted to steganalysis algorithm determining presence a secret message embedded into digital image which is stored in compressed or uncompressed form. The algorithm is based on the analysis of pairs of colors and uses the method of modifying the least significant bit.

Keywords: steganography, steganalysis, close-color pairs, unique colors, information hiding

Mathematics Subject Classification (2010) 93A30

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 2, pp. 190-195

RESEARCH OF MAJOR INFORMATION TASKS SOLVED BY THE MATHEMATICAL MODELING OF DIFFUSION PROCESSES

Muayad Omar Abdullah, Anatoly A. Berezovsky

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: omarukrain@yahoo.com

The multimedia information technology to implement tools of mathematical modeling in anomalous diffusion processes are considered. The basic information tasks are studied and the basic requirements for information technology, focused on solving the problems of mathematical modeling are analyzed.

Keywords: multimedia information technology, diffusion process, mathematical modeling, numerical experiment

Introduction

The main set of problems being solved in the mathematical modeling, comprises the development of mathematical models (MM) processes being studied and the development of computational and numerical methods of implementing these MM. In this case, as a rule , the conservation laws (of mass, energy, momentum, etc.) which derive the dynamic equations, initial and boundary conditions (the essence is MM) are studied; the analytical and numerical methods for solving the dynamic equations are developed ,as well as the qualitative properties received as a result of the solutions (the research of existence, uniqueness, convergence and accuracy of the solutions; the definition of computational costs of the solutions, carrying out testing of the proposed MM, etc.).

However, there should be also recognized the important issues related to the presentation obtained through the solutions of the mathematical modeling. First of all, this aspect relates to the use of information technology (IT) and is associated with the submission, analysis and implementation of the solutions obtained.

The aim of the work

The aim of this work is identification and analysis of the basic requirements for the information technology oriented to presenting the results of the mathematical modeling in the diffusion (including the so-called «anomalous») processes.

The main part

The problems arising (as noted above) in interpreting the results of the mathematical modeling consist in the following. In a number of important practical cases in the mathematical modeling the diffusion processes (DP) are considered as processes with distributed parameters. The spatial area of RP processes in the simulation is a finite grid nodes [1–3] or finite elements [4, 5], and the function of the state an array of values of the grid functions at these nodes (or functions in finite elements). Depending on the desired accuracy of the solution, obtained grid functions array (in finite elements) have considerable

dimensions ($10^2 - 10^5$ values). Considering such quantity of values the possibilities to interpret the solutions become of paramount importance (for example, the ordering of arrays of values and form of presentation, methods of storage and handling, conversion, etc.).

In addition, the results of mathematical modeling are often only an intermediate link in the solved application problem. For example, in solving problems of technological or natural processes control (technical objects) as a result of mathematical modeling receive function of the state of the object on which (taking into account the control law) control action is synthesized. Thus, usually, the control action synthesis must be manipulated in real (or even accelerated) time-scale in the case of solutions of optimization or multivariate tasks. Given the fact that the technological or natural processes (technical facilities), as noted earlier, primarily represent RP processes (RP-objects) (with their inherent features and complexities of mathematical modeling and above all – the considerable size of arrays that define the values of state function), the rational methods of data processing is a priority. In these circumstances, the IT oriented to development and application of methods and tools for processing the results of mathematical modeling are relevant scientific and applied technical problem.

Implementation of computer simulations in the practice of theoretical studies and a wide range of data processing technology has solved fundamentally new problems, and, in some cases, has led to the emergence of new domains, the existence of which was not possible before the appearance of modern computer technology (CT) and the development of IT. Formation of a broad class of modern theoretical and applied areas of research (such as those associated with the atmosphere, mining and other physically complex processes and facilities that are experiencing a certain kind of diffusion anomalies) was fully possible only thanks to the emergence of computer simulation. Examples of the most important areas of research in which mathematical (computer) modeling plays a major role, are, in particular, the problem of numerical weather prediction, climate change, and issues related to air pollution and other environmental components.

The need for the use of IT, in this case, is due to several reasons:

- the equations that describe the various processes that can not be solved analytically without using numerical methods, the implementation and interpretation of which are due to the use of IT tools;
- modeling of this class of processes related to the huge amount of computation, often requiring the use of the most powerful computational tools and advanced IT;
- the only experimental data on the state of the complex processes are the data of many observations (for example, for geological processes is well-drilling and measurement of reservoir pressure in them; for processes in the atmosphere is the definition of the characteristics of it condition by ground stations, weather balloons, aircraft, various systems remote sensing based on ground-based radars and satellites in orbit), and the assimilation of such an extensive set of data from different sources is not possible without the use of modern processing systems, data collection and transmission of information;
- conducting simulations (including mathematical) involves the manipulation of large size of intermediate data and analysis (for example, ordering the long-term prognosis, etc.) of the obtained results, the effective carrying out of which is not possible without the use of various IT;
- series of mathematical modeling (especially in the field of regional and global climate seismic surveying and geo-ecology; variational data assimilation of complex technological processes) is the need to maintain huge data archives, regular and effective access to which is to be provided by means of IT.

If we consider the mathematical modeling in conjunction with implementing its IT, then, in this case, it is permissible to speak of information and mathematical modeling (MI-simulation) [4, 6]. The process of MI-simulation includes: gathering the necessary information (in accordance with the intended purpose), component (determining) the

information model of the process (object) processing of the data (their organization or structuring) and the algorithm to convert the data (encapsulation), the formation of MM process (object); geometrization of the model or the results of its numerical implementation (computer visualization using computer graphics – perform geometric constructions).

Thus, we can conclude that for solving mathematical modeling problems the IT provide the preparation (and if necessary, collection, such as in the case of atmospheric modeling) source data and interpret the results of the solution in a convenient form or, more generally, act as an IT tool implementation methods and mathematical modeling, accounting, in conjunction with the latter, the basis of MI-simulation in which IT resources and mathematical modeling of the most effective complement each other in the course of solving applied problems.

Typical information technology structure, focused on solving the problems of mathematical modeling. The most important factor in determining the effectiveness of IT is its structure (i.e., the elements that make up the IT and topological relationships between them).

Academician A. Samarskiy proposed IT [6, 7], the structure of which (Fig. 1) best meets the objectives of mathematical modeling solutions. The structure of the IT presented in the form of a triad «Model — Algorithm — Program» is uniquely defined plan of action using the methods of mathematical modeling:

- select (or construct) «equivalent» object reflecting in mathematical form, its most important properties - laws to which it is subject, communications inherent in its constituent parts, etc. (In other words, the essence MM);
- selection (or development) of the algorithm for implementation of the model on the computer;
- the creation of programs, «transforming» the MM algorithm and an available computer language.

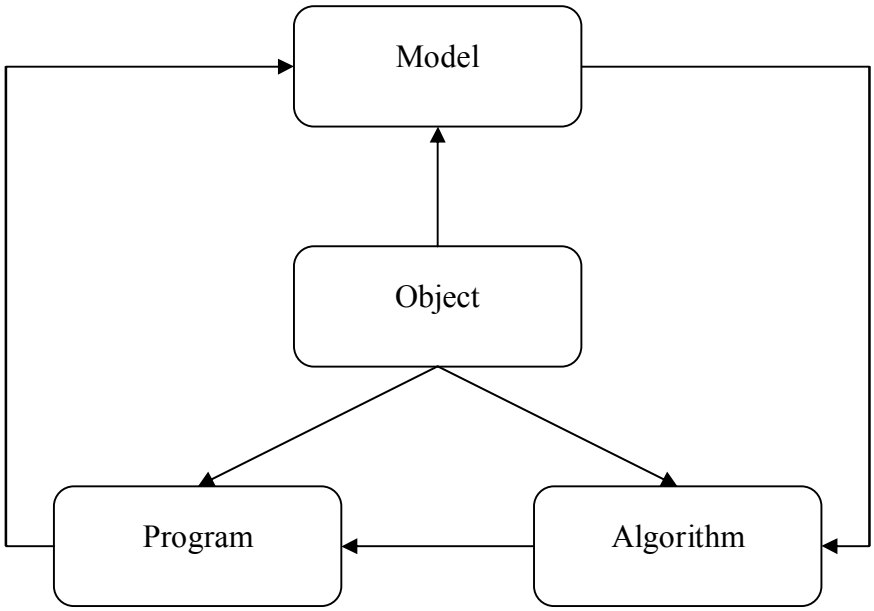


Fig. 1. The structure of IT oriented to solve mathematical modeling problems (typical structure)

About the properties of this structure is necessary to note the following. MM as the most important element of the triad should be adequate to the object under study (the process). This should be confirmed by an experiment of some kind (i.e., the «behavior» of the real object (process) and MM under the same conditions should be the same). After

establishing the adequacy of the triad of the original object with MM held a variety of «experiments»: computational experiments that provide all of the required quality and quantity of the properties and characteristics of the object (process). Computational experiment is designed to study, forecasting, optimization of complex (including multi-parameter and nonlinear objects (processes)), which theoretical and experimental research with traditional methods is difficult.

Computational experiment, in contrast to the experiments on full-scale objects (processes) can accumulate the results obtained in the study of a variety of problems, and then quickly and flexibly to apply them to solve problems in completely different areas. This property has a «universal» MM formalizing the majority of PD. For example, the nonlinear heat equation is suitable for describing not only the thermal processes, but also the diffusion of matter, the movement of ground water, gas filtration in porous media. Changes only the physical meaning of the quantities in this equation. The modeling process is accompanied by the improvement and refinement, as appropriate, all parts of the triad.

It should be noted that the current state of CT and modern numerical methods performs simulations of objects that describe the behavior of highly complex mathematical relations, such as non-linear systems of differential or integral equations. But the complex computational algorithms have their own internal properties, which are not always similar, even up to the error of approximation, the properties of the original MM. This may give rise to effects that are purely computational nature. Therefore, an important problem in the theory of numerical methods is (in relation to the structure under consideration IT) development of computational algorithms that exclude or minimize the occurrence of such situations. The problem of developing adequate MM to describe the various DP, as well as methods of implementing, remains relevant. An important role in this triad play programs realizing computational algorithms. They need to ensure the effectiveness of the solution of a mathematical problem with a minimum of computational effort.

Thus, IT, supporting computational experiment in the structure include: methods of construction of the MM information support to the implementation of recent search and selection algorithms and software for the numerical solution of problems, methods and control of accuracy and correctness of calculations made of the applicable programs.

Given the above, the structure IT, shown in Fig. 1, can be taken as a typical model (generalized), which is focused on solving the problems of mathematical modeling, as it covers all the main aspects of the solution of this class of problems. On the basis of the typical structure of IT the IT structure are formed, intended for applications of mathematical modeling.

Analysis of the basic requirements for information technology, focused on solving the problems of mathematical modeling of diffusion processes

Obviously, the IT solution providing a particular class of mathematical modeling (in particular, simulation of diffusion processes) must meet certain requirements. These requirements reflect the connection between the main (basic) properties studied in the mathematical modeling of objects, processes and phenomena with the means used by IT and, ultimately, determine the effectiveness of the latter.

Let’s perform the analysis of the basic requirements for solving an IT-oriented problems of mathematical modeling of diffusion processes. Considering the mathematical modeling of diffusion processes, include the following requirements to the basic ones:

- the ability to handle the significant volume of arrays of numeric information, which is the field values of the unknown functions for the DP state. Moreover, this manipulation is to provide both a multi-dimensional array operations (mainly two-and three-dimensional) and the ability to obtain results in real (or even accelerated) time scale, taking into account the subsequent decision of multivariate optimization and control tasks;

- the ability to adequately reflect the qualitative dynamic behavior of DP at the stage of visualizing the solutions for mathematical modeling, taking into account mainly the distributed nature of the processes under study. In other words, when rendering the solutions received (or displayed) by this or that IT the former should adequately, i.e. up to the full-scale experiments on the real object (process) reflect its dynamic behavior considering the effect on of external disturbances and control on the object (process);
- the establishment of the effective (in terms of the computational cost) numerical methods for implementing the mathematical modeling of the DP in IM modeling procedures. The complexity of formalizing the problems of mathematical modeling in the DP imposes higher demands on the computational costs for the machine implementation of the methods applied in the use of IT for numerical study of DP, due to, in particular, the ultimate non-representability of the MM in DP, non-trivial character of spatial modeling and boundary conditions. Eventually, the computational costs for implementing the mathematical modeling methods determine the effects of these techniques (as part of the MI-simulation technology) under the specified criteria;
- the ability to automate the process of mathematical modeling in DP. That is, IT must ensure that the «liberation» of the man-researcher from unproductive labor-intensive operations of the computing process (for example, the task of geometry and spatial sampling areas, the definition of the parameters of discrete spatial regions, counting these parameters while solving the time-dependent and non-linear problems, task, counting and entering the initial and boundary conditions, etc.), leaving the man-researcher if necessary the function analysis and decision making based on the results of mathematical modeling.

Conclusion

The basic requirements to an IT oriented to problem solving of mathematical modeling in diffusion processes are presented. Possible ways of improving the effectiveness of IT in the applied research are described, as well as, the possibility of interpreting the structure of a typical IT to solve scientific and engineering problems is analyzed.

References

1. Верлань, А.Ф. Математическое моделирование аномальных диффузионных процессов [Текст] : монография / А.Ф. Верлань, С.А. Положаенко, Н.Г. Сербов. — К.: Наукова думка, 2011. — 416 с.
2. Бусленко, Н.П. Моделирование сложных систем [Текст] : научное издание / Н.П. Бусленко. — М. : Наука, 1968. — 356 с.
3. Коздоба, Л.А. Электрическое моделирование явлений тепло- и массопереноса [Текст] : научное издание / Л.А. Коздоба. — М. : Энергия, 1972. — 296 с.
4. Згуровский, М.З. Прикладные методы анализа и управления нелинейными процессами и полями [Текст] : монография / М.З. Згуровский, В.С. Мельник, А.Н. Новиков ; НАН Украины. Ин-т прикл. сист. анализа. Нац. техн. ун-т Украины «Киевск. политехн. ин-т». — К. : Наук. думка, 2004. — 588 с.
5. Мацевитый, Ю.М. Моделирование нелинейных процессов в распределенных системах [Текст] : монография / Ю.М. Мацевитый, В.Е. Прокофьев ; Акад. наук УССР. — К. : Наук. думка, 1985. — 304 с.
6. Самарский, А.А. Компьютеры и жизнь. Математическое моделирование [Текст] : научно-популярная литература / А.А. Самарский, А. П. Михайлов ; гл. ред. И.В. Петрянов. — Москва : Педагогика, 1987. — 128 с.

7. Самарский, А.А. Математическое моделирование. Идеи. Методы. Примеры [Текст] : монография / А.А. Самарский, А.П. Михайлов. — 2-е изд., испр. — М. : Физматлит, 2001. — 316 с.

ДОСЛІДЖЕННЯ ОСНОВНИХ ІНФОРМАЦІЙНИХ ЗАДАЧ, ЯКІ ВИРІШУЮТЬСЯ ПРИ МАТЕМАТИЧНОМУ МОДЕЛЮВАННІ ДИФУЗІЙНИХ ПРОЦЕСІВ

Омар Муааяд Абдуллах, А.А. Березовський

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: omarukrain@yahoo.com

Розглядається мультимедійна інформаційна технологія реалізації засобів математичного моделювання аномальних дифузійних процесів. Досліджено основні інформаційні задачі та виконано аналіз базових вимог щодо інформаційних технологій, які орієнтовано на розв'язання задач математичного моделювання.
Ключові слова: мультимедійна інформаційна технологія, дифузійний процес, математичне моделювання, обчислювальний експеримент

ИССЛЕДОВАНИЕ ОСНОВНЫХ ИНФОРМАЦИОННЫХ ЗАДАЧ, РЕШАЕМЫХ ПРИ МАТЕМАТИЧЕСКОМ МОДЕЛИРОВАНИИ ДИФФУЗИОННЫХ ПРОЦЕССОВ

Омар Муааяд Абдуллах, А.А. Березовский

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: omarukrain@yahoo.com

Рассматривается мультимедийная информационная технология реализации средств математического моделирования аномальных диффузионных процессов. Исследованы основные информационные задачи и выполнен анализ базовых требований к информационным технологиям, ориентированных на решение задач математического моделирования.
Ключевые слова: мультимедийная информационная технология, диффузионный процесс, математическое моделирование, вычислительный эксперимент

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 3, номер 1, 2013. Одеса – 98 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 3, номер 1, 2013. Одесса – 98 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 3, No. 1, 2013. Odesa – 98 p.

Засновник: Одеський національний політехнічний університет

Зареєстровано Міністерством юстиції України 04.04.2011р.

Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Одеського національного політехнічного університету (протокол №7 від 30.04.2013)

Адреса редакції: Одеський національний політехнічний університет,

проспект Шевченка, 1, Одеса, 65044 Україна

Web: http://www.immm.opu.ua

E-mail: immm.ukraine@gmail.com