МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 2, № 1

Volume 2, No. 1

Одеса – 2012
Odesa – 2012

Інформатика та математичні методи в моделюванні
Науковий журнал
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*

Informatics and mathematical methods in simulation
Scientific journal
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 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 1, pp. 5-17

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СОКРЫТИЯ ИНФОРМАЦИИ ДЛЯ СИСТЕМ С ЗАШУМЛЕННЫМИ КАНАЛАМИ СВЯЗИ

И.И. Маракова[1], А.А. Яковенко[2]

[1] Telecom Bretagne,
Technopôle Brest-Iroise, CS 83818, 29238 Brest Cedex 3, France; e-mail: marakova.irina@gmail.com
[2] Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: iakovenko.oleksandr@gmail.com

Рассматривается система передачи сокрытой информации по зашумленным каналам связи и сценарий, при котором атакующая сторона не имеет другого доступа к стеганосигналу, кроме как в гауссовом канале. При таком подходе требуется обеспечить практически недостижимую на практике величину отношения сигнал/шум, особенно с учетом того, что покрывающее сообщение может быть известно атакующей стороне. Для решения этой проблемы предлагается использовать стеганосистему с разнесением по времени (СРВ). Доказана возможность построения СРВ с заданным уровнем секретности и надежности восприятия сокрытого сигнала. Рассмотрены вопросы оптимизации параметров на основе использования кодов коррекции ошибок. Представлены результаты моделирования при помощи реализации СРВ для покрывающих сообщений в виде цифровых звуковых файлов формата WAV.

Ключевые слова: стеганосистема, покрывающее сообщение, коды коррекции ошибок, гауссовский канал с шумами, относительная энтропия

Введение

Стеганография – это техника сокрытия информации, позволяющая добавить скрытую информацию в не вызывающее подозрения покрывающее сообщение (аудио-, видеоинформация и т.д.) при условии, что покрывающее сообщение (ПС) не искажается до такой степени, что может сделать заметным наличие в стеганосигнале дополнительной информации.

Для обеспечения устойчивости к статистическим атакам необходимо обеспечить идентичность вероятностных мер ПС и стегосигнала на некотором временном дискрете. Но для реализации этого принципа разработчик стегосистемы должен, по меньшей мере, владеть информацией о статистике ПС, т.е. реального аудио или видеосигнала, что само по себе является довольно сложной задачей. С целью решения этой проблемы и было предложено построение стегосистемы на основе каналов с зашумлением [1].

Известно направление развития методов передачи конфиденциальной информации по незащищенным каналам связи с шумом при достаточно низкой сложности реализации и малых финансовых затрат, гарантирующее сколь угодно малую вероятность успешного перехвата и сколь угодно малую вероятность ошибки в канале легитимных пользователей [2]. Применение данного подхода в стеганографии может быть оправдано только при наличии естественного зашумленного канала и только в том случае, когда атакующая сторона не имеет другого доступа к стегосигналу, кроме как в зашумленном канале. Суть атаки заключается в выявлении сокрытого сообщения на

основе анализа вероятностных мер перехваченного сигнала. Необходимо отметить, что такая модель является более жесткой, чем стандартная стеганосистема, для которой ПС в большинстве случаев является известным. Таким образом, проблема стеганоанализа сводится к выделению из канального шума внедренного скрытого сообщения. Так как распределение шума в канале, как правило, известно намного лучше, чем статистика ПС, проблема разработки стегосистемы упрощается.

В статье рассматривается только гауссовский канал [1]. Если для стегосистемы информационную ценность представляют как ПС, так и скрываемая информация, т.е. внедряемая информация является цифровым водяным знаком (ЦВЗ), то внедрение бита информации может быть реализовано как:

$$\forall n = 1,\ldots,N : C_W(n) = C(n) + (-1)^b \sigma_W \pi(n), \tag{1}$$

где

$C = (C(n))_{n=1}^N$ – ПС;

$\pi = (\pi(n))_{n=1}^N$ – независимые одинаково распределенные по закону Гаусса псевдослучайные величины с нулевым средним значением и единичной дисперсией;

N – длина обеих последовательностей;

σ_W – дисперсия ЦВЗ.

На выходе гауссовского канала получим:

$$\forall n = 1,\ldots, N : C'_W(n) = C_W(n) + \varepsilon(n),$$

где $\varepsilon = (\varepsilon(n))_{n=1}^N$ – независимый одинаково распределенный по закону Гаусса шум с нулевым средним значением и дисперсией σ_ε^2.

Как было показано, относительная энтропия для данной модели стегосистемы даже в случае известного ПС может быть представлена [1], [3] как:

$$D = 0.72N\left[\ln\left(1+\frac{1}{\eta_W}\right) - \frac{1}{1+\eta_W}\right], \tag{2}$$

где $\eta_W = \sigma_\varepsilon^2 / \sigma_W^2$ – отношение дисперсий гауссовского шума и ЦВЗ.

Для того чтобы надежно спрятать секретную информацию в шуме канала, отношение η_W должно быть большим [3]. Следовательно, относительная энтропия (2) приближенно равна

$$D \approx 0.36\frac{N}{\eta_W^2}. \tag{3}$$

Из теории информации известно, что инвариантно к методу статистического анализа должно выполняться неравенство:

$$P_{ЛД}\ln\frac{P_{ЛД}}{1-P_{ПС}} + (1-P_{ЛД})\ln\frac{1-P_{ЛД}}{P_{ПС}} \le D, \tag{4}$$

где

$P_{ЛД}$ – вероятность ложного детектирования стегосигнала,

$P_{ПС}$ – вероятность пропуска стегосигнала.

Допустим для простоты изложения, что $P_{ЛД} = P_{ПС} = P$. Тогда из (4) получаем

$$(2P-1)\ln\frac{P}{1-P} \le D.$$

Из (3) следует, что:

$$\eta_W = 0.6\sqrt{\frac{N}{D}}. \tag{5}$$

Оптимальным правилом принятия решения о наличии/отсутствии сокрытого бита b для гауссовского канала и информированного декодера, т.е. такого декодера, которому известно ПС, является:

$$\Lambda = \sum_{n=1}^{N}\left(C'(n)-C(n)\right)\pi(n) \Rightarrow \widetilde{b} = \begin{cases} 0, \text{ если } \Lambda \ge 0 \\ 1, \text{ в противном случае} \end{cases}. \tag{6}$$

Нетрудно показать, что для гауссовской последовательности $\pi = \left(\pi(n)\right)_{n=1}^{N}$ вероятность принятия неправильного решения (6) имеет следующий вид:

$$P_{ош} = \Phi\left(\sqrt{\frac{N}{\eta_W + 2}}\right) \le \exp\left(-\frac{N}{2(\eta_W + 2)}\right), \tag{7}$$

где $\Phi : x \mapsto \Phi(x) = \frac{1}{\sqrt{2\pi}}\int_x^{+\infty} e^{-\frac{u^2}{2}}du$.

Если $\eta_W >> 1$, что является довольно обычным для стеганосистем, то требование к секретности сводится к следующему выражению:

$$P_{ош} = \Phi\left(\sqrt{\frac{N}{\eta_W + 2}}\right) \le \exp\left(-0.83(ND)^{\frac{1}{2}}\right). \tag{8}$$

Из (8) следует важный вывод, что для любого уровня надежности восприятия и значения D может быть выбрано значение N, обеспечивающее требуемый уровень секретности, т.е. заданное значение $P_{ош}$.

При практической реализации данного подхода очевидно следующее противоречие. Для уменьшения вероятности ошибки извлечения ЦВЗ легальным пользователем, необходимо увеличить параметр η_W, что неизбежно ведет к увеличению искажений стегосигнала, т.е. уменьшению надежности восприятия. Для устранения данного противоречия и применяется так называемая стеганосистема с разнесением по времени.

Далее будет приведено ее описание и рассмотрены возможности оптимизации ее параметров на основе применения кодов коррекции ошибок, а также представлены результаты симуляции для цифрового звукового сигнала формата WAV в качестве ПС.

Описание стеганосистемы и оценка ее эффективности

Для стегосистемы с разнесением по времени без кодирования (рис. 1) правило (1) внедрения секретных бит преобразуется к виду:

$$\Pr[C_W(n) = C(n) + (-1)^b \sigma_W \pi(n)] = P_0,$$
$$\Pr[C_W(n) = C(n)] = 1 - P_0. \quad (9)$$

Для практической реализации модифицированного правила внедрения (9) используемая псевдослучайная последовательность отсчетов может быть непосредственно секретным ключом (СК) или может быть связана с СК по некоторому закону. Пусть $(n_m)_{m=1}^{N_s}$ – последовательность увеличивающихся индексов $(N_s \le N)$, определяющая номера отсчетов, в которые будет производиться внедрение стегосигнала (рис. 1). Для большого значения N, с учетом центральной предельной теоремы, $P_0 = N_s / N$. При отсутствии кодирования для внедрения секретного бита b используется N_0 последовательно выбранных дискретов для погружения ЦВЗ. Отсюда следует, что общее количество секретных бит составит $N_t = N_s / N_0$. Каждый легальный пользователь должен знать стеганоключ K, другими словами – номера отсчетов с внедренным ЦВЗ, и способен выделить по одному все N_t секретных бит, используя правило принятия решений (6). Вероятность ошибки может быть найдена из (7) путем подстановки в формулу текущего значения N_0 вместо N.

Атакующая сторона, при условии известного ПС, но при неизвестном СК, для принятия решения о наличии или отсутствии сокрытого сообщения должна выполнить статистический анализ и протестировать две гипотезы:

$$H_0 : [C''(n) \in N(0, \sigma_\varepsilon^2) \text{ и является ППС}], \quad (10)$$

$$H_1 : \begin{cases} \Pr[C''(n) \in N(0, \sigma_s^2) \text{ и является ППС}] = P_0, \\ \Pr[C''(n) \in N(0, \sigma_\varepsilon^2) \text{ и является ППС}] = 1 - P_0, \end{cases} \quad (11)$$

где

$C''(n) = (C'_W(n) - C(n))_{n=1}^{N}$;

$\sigma_s^2 = \sigma_\varepsilon^2 + \sigma_W^2$;

ППС – псевдослучайная последовательность некоррелированных чисел.

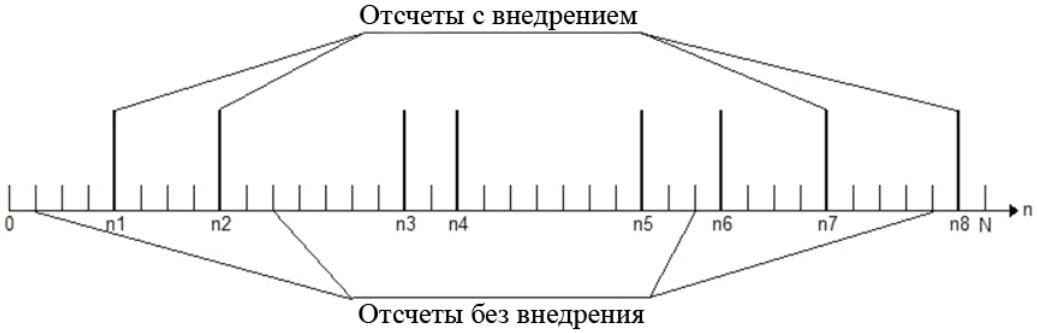

Рис. 1. Псевдослучайные отсчеты для СРВ, $N_s = 8,\ N = 38,\ P_0 = 4/19$

Проверка гипотез может осуществляться путем вычисления отношения максимального правдоподобия:

$$\Lambda\left(\Lambda_1|\Lambda_0\right)=\frac{P\left(C''(n)|H_1\right)}{P\left(C''(n)|H_0\right)}, \tag{12}$$

где $P\left(C''(n)|H_j\right)$ – вероятность распределения случайной величины $C''(n)$ для каждой из гипотез H_j, $j=0,1$. Проверка оптимальной гипотезы, основанной на отношении максимального правдоподобия (12), выглядит следующим образом:

$$\begin{aligned}&\Lambda\left(\Lambda_1|\Lambda_0\right)\geq\lambda\Rightarrow H_1,\\&\Lambda\left(\Lambda_1|\Lambda_0\right)<\lambda\Rightarrow H_0,\end{aligned} \tag{13}$$

где λ – некоторый фиксированный порог. Подставив в (13) распределения вероятности (10), (11), получим после простых преобразований:

$$\Lambda\left(\Lambda_1|\Lambda_0\right)=\prod_{n=1}^{N}\left[P_0\sqrt{\frac{\sigma_\varepsilon^2}{\sigma_s^2}}\exp\left(\frac{\sigma_W^2}{2\sigma_s^2\sigma_\varepsilon^2}\left(C''(n)\right)^2\right)+\left(1-P_0\right)\right],$$

или для логарифмического масштаба

$$\Lambda_L\left(\Lambda_1|\Lambda_0\right)=\log\Lambda\left(\Lambda_1|\Lambda_0\right)=\sum_{n=1}^{N}\log\left[P_0\sqrt{\frac{\sigma_\varepsilon^2}{\sigma_s^2}}\exp\left(\frac{\sigma_W^2}{2\sigma_s^2\sigma_\varepsilon^2}\left(C''(n)\right)^2\right)+\left(1-P_0\right)\right]. \tag{14}$$

Применение на практике полученного правила принятия решений (14) довольно сложно. Рассмотрим подоптимальное правило принятия решений в случае выполнения условия $\sigma_W^2<<\sigma_\varepsilon^2$. При этом (14) преобразуется к виду

$$\frac{1}{N}\sum_{n=1}^{N}\log\left[P_0\exp\left(\frac{1}{2\eta_W^2\sigma_\varepsilon^2}\left(C''(n)\right)^2\right)+\left(1-P_0\right)\right]. \tag{15}$$

При $x\mapsto\log(1+x)$ получим:

$$\Lambda_L\left(\Lambda_1|\Lambda_0\right)=P_0\left[\sum_{n=1}^{N}\exp\left(\frac{1}{2\eta_W^2\sigma_\varepsilon^2}\left(C''(n)\right)^2\right)-N\right]$$

и правило принятия решений:

$$[\widetilde{\Lambda}\geq\widetilde{\lambda}\Rightarrow H_1];\qquad[\widetilde{\Lambda}<\widetilde{\lambda}\Rightarrow H_0], \tag{16}$$

где

$\widetilde{\Lambda}=\frac{1}{\mathrm{N}}\sum_{n=1}^{N}\left(C''(n)\right)^2$;

$\widetilde{\lambda}$ – некий новый порог.

Правило принятия решений (16) достаточно обосновано, поскольку, как будет показано далее $M[(C''(n))^2|H_1] > M[(C''(n))^2|H_0]$, где M – математическое ожидание.

Рассмотрим аналитическую оценку вероятностей ошибок первого и второго рода, $P_{ПС}$ и $P_{ЛД}$ соответственно, для гипотезы H_1 (наличие стегосигнала) и гипотезы H_0 (отсутствие стегосигнала) при использовании правила принятия решений (16).

Для достаточно больших N, согласно центральной предельной теореме [3], $\tilde{\Lambda} \in N(\mu_j, \sigma_j^2)$ для H_j, где $\mu_j = M[\tilde{\Lambda}|H_j]$, и $\sigma_j^2 = Var(\tilde{\Lambda}|H_j)$, для $j = 0,1$. Так как $\sigma_1^2 > \sigma_0^2$, получим:

$$P_{ПС} \geq \frac{1}{\sqrt{2\pi\sigma_0^2}} \int_{-\infty}^{\tilde{\lambda}} \exp\left(-\frac{(x-\mu_1)^2}{2\sigma_0^2}\right) dx, \tag{17}$$

$$P_{ЛД} \geq \frac{1}{\sqrt{2\pi\sigma_0^2}} \int_{\tilde{\lambda}}^{+\infty} \exp\left(-\frac{(x-\mu_1)^2}{2\sigma_0^2}\right) dx. \tag{18}$$

Выберем порог $\tilde{\lambda}$ таким образом, чтобы выполнялось условие $P_{ПС} = P_{ЛД} = P$. После простых преобразований выражений (17) и (18), можно получить неравенство:

$$P \geq \Phi\left(\frac{\mu_1 - \mu_0}{2\sigma_0}\right) \tag{19}$$

при выполнении условий

$$\mu_0 = \sigma_\varepsilon^2; \quad \mu_1 = \sigma_\varepsilon^2 + P_0\sigma_W^2; \quad \sigma_0^2 = \frac{2}{N}\sigma_\varepsilon^4. \tag{20}$$

Подставив (20) в (19), получим:

$$P \geq \Phi\left(\sqrt{\frac{N}{2}\frac{P_0}{2\eta_W}}\right),$$

или

$$P \geq \Phi\left(\frac{N_s}{2\sqrt{2N}\eta_W}\right).$$

Следовательно, если асимптотически $N_s \sim \sqrt{N}$, то $P \sim 1/2$, что приводит к невозможности обнаружения стегосигнала нелегитимным пользователем.

Для внедрения m секретных бит в N_s отсчетов необходимо выбрать $N_0 = \frac{N_s}{m}$ отсчетов для каждого бита секретного сообщения. В таком случае вероятность ошибки $P_{ош}$ после извлечения одного бита легальным информированным декодером определяется по (7) (с подстановкой N_0 вместо N). Необходимо заметить, что для того, чтобы выделить секретные биты, декодер легитимного пользователя должен быть синхронизирован как с последовательностью π в (1), так и с псевдослучайной

последовательностью, определяющей номера отсчетов, в которые производилось внедрение, т.е. СК.

В табл. 1 показаны результаты вычисления для некоторых значений параметров N_s, N_0, m и P_0, позволяющие достигнуть $P_{ош} \le 10^{-3}$ и $P \ge 0.4$, с заданными значениями N и η_W, отвечающими требованиям надежного восприятия. Для достаточно больших N становятся возможными высокая скрытность ($P \ge 0.4$) и устойчивость ($P_{ош} \le 10^{-3}$) СРВ при погружении до 232 бит защищенной информации.

Таблица 1.

Наборы параметров для СРВ, обеспечивающие $P_0 \ge 0.4$ и $P_{ош} \le 10^{-3}$ при разных значениях N и η_W

N	η_W	N_0	N_s	m	P_0
10^4	20	210	1431	6	0.1431
	50	496	3578	7	0.3578
	100	973	7156	7	0.7156
10^5	20	210	4526	21	0.04526
	50	496	11310	22	0.1131
	100	973	22630	23	0.2263
10^6	20	210	14310	68	0.01431
	50	496	35780	72	0.03578
	100	973	71560	73	0.07156
10^7	20	210	45260	215	0.004526
	50	496	113100	228	0.01131
	100	973	226300	232	0.02263

Для улучшения эффективности СРВ можно использовать СРВ с кодированием. Тогда процедура внедрения (9) должна быть модифицирована следующим образом. Для заданного ПС $C = (C(n))_{n=1}^{N}$ пусть $C_w = (C_W(n))_{n=1}^{N}$ и для каждого индекса n_j при внедрении стегосигнала будет выполняться

$$\Pr\left[C_W(n_j) = C(n_j) + (-1)^{b_{ij}} \sigma_W \pi(n_j)\right] = P_0,$$

$$\Pr\left[C_W(n_j) = C(n_j)\right] = 1 - P_0,$$

где

b_{ij} – это *j*-й бит в *i*-ом кодовом слове длины $N_0 = N_s / \ell$,

ℓ – положительное целое число.

Для простоты изложения ограничимся рассмотрением бинарных линейных систематических (N_0, k, d)-кодов, изменяя i в интервале $\{1,2,\cdots,2^k - 1, 2^k\}$, где d – минимальное кодовое расстояние. Информированный декодер принимает решение о внедрении *i*-го кодового слова стеганосообщения, вычисляя

$$i = \arg\max_{1 \le i' \le 2k} \sum_{j=1}^{N_0} \left(C'_W(n_j)\right)(-1)^{b_{i'j}} \pi(n_j).$$

Полное количество внедренных бит $m = kl$, и вероятность ошибочного блока $P_{ОБ}$, основываясь на хорошо известной границе неравенства Буля [5], может быть выражена следующим образом:

$$P_{ОБ} \le \left(2^k - 1\right)\Phi\left(\sqrt{\frac{d}{2+\eta_W}}\right) \le \exp\left(-\frac{d}{2\left(2+\eta_W\right)} + RN_0 \ln 2\right).$$

Так как отношение сигнал/шум η_W^{-1} обычно мало, ограничимся лишь двумя классами линейных кодов коррекции ошибок: симплексными кодами (СК) и кодами Рида-Маллера (КРМ) [5]. Для первого класса основные параметры – $N_0 = 2^\nu - 1$, $k = \nu$, $d = 2^{\nu-1}$, $R = \frac{\nu}{N_0}$, где ν – некоторое целое число; для второго класса – $N_0 = 2^\nu$, $k = \sum_{i=1}^{r}\binom{\nu}{i}$, $d = 2^{\nu-r}$, где $\nu \ge 3$ и r – целое число, т.н. порядок КРМ.

Теперь можно зафиксировать полное количество отсчетов N, уровень защищенности P, вероятность ошибки в блоке $P_{ОБ}$, параметр η_W, а затем оптимизировать параметры кода N_0, ν и r с целью увеличения числа защищенных и достоверных бит.

Например, если задаться значениями $N = 10^7$, $P \ge 0.4$, $P_{ОБ} \le 10^{-3}$, $\eta_W = 20$, то оптимальными параметрами СК будут $\nu = 10$, $k = 10$, а общее число внедряемых секретных бит $m = k\frac{N_s}{N_0} = 442$.

Если требуется усилить надежность системы, можно использовать КРМ с оптимальными параметрами $\nu = 14$, $r = 2$, $k = 105$ и с теми же ограничениями $P \ge 0.4$, $\eta_W = 20$. В таком случае общее число внедренных секретных бит будет близко к 290 при $P_{ОБ} \le 10^{-9}$.

Таким образом, использование кодов коррекции ошибок позволяет увеличить число внедряемых защищенных бит и/или повысить секретность системы.

Определим, может ли правило принятия оптимального решения (14) обеспечить значительные улучшения при детектировании в СРВ по сравнению с субоптимальным правилом принятия решений (15).

Так как N значительно больше, можно применить центральную предельную теорему к сумме из (15). Тогда, аналогично доказательству выражения (19), можно получить такой критерий выбора порога λ, который позволяет достичь для $P_{ПС} = P_{ЛД} = P$ следующей верхней границы:

$$P \ge \Phi\left(\frac{\widetilde{\mu}_1 - \widetilde{\mu}_0}{2\widetilde{\sigma}_0}\right), \qquad (21)$$

где для $j = 0,1$

$$\widetilde{\mu}_j = M\left[\left(\log\left(P_0 \exp\left(\frac{\left(C''(n)\right)^2}{2\eta_W\sigma_\varepsilon^2}\right) + \left(1 - P_0\right)\right)\right)_{n=1}^{N} \middle| H_j\right]$$

и

$$\widetilde{\sigma}_0 = \frac{1}{N} Var\left(\left(s(n)\right)_{n=1}^{N} \middle| H_j\right) = \frac{1}{N}\left(M\left[\left(s^2(n)\right)_{n=1}^{N} \middle| H_j\right] - \widetilde{\mu}_0^2\right),$$

где $s(n) = \log\left(P_0 \exp\left(\frac{\left(C''(n)\right)^2}{2\eta_W \sigma_\varepsilon^2}\right) + \left(1 - P_0\right)\right)$, и случайные значения $C''(n)$ имеют вероятность распределения, приведенную в (10). Так как крайне сложно определить значения $\widetilde{\mu}_0$, $\widetilde{\mu}_1$ и $\widetilde{\sigma}_0$ аналитически, они будут оценены в результате симуляции описанной выше процедуры.

В табл. 2 представлены результаты симуляции для $\widetilde{\mu}_0$, $\widetilde{\mu}_1$ и $\widetilde{\sigma}_0$, а также результаты вычисления P из (21) для типичных значений σ_ε^2, η_W и P_0. Очевидно, что использование правила оптимального решения не нарушает секретность СРВ (P), следовательно, последняя может считаться защищенной стеганосистемой.

Таблица 2.

Результаты симуляции значений $\widetilde{\mu}_0$, $\widetilde{\mu}_1$ и $\widetilde{\sigma}_0$ в зависимости от типичных значений σ_ε^2, η_W и P_0

N	σ_ε^2	η_W	$P_0 = N_s / N$	$\widetilde{\mu}_0$	$\widetilde{\mu}_1$	$\widetilde{\sigma}_0$	$P = Q\left(\frac{\widetilde{\mu}_1 - \widetilde{\mu}_0}{2\widetilde{\sigma}_0}\right)$
10^4	1	20	0.1431	0.00161414	0.00162667	0.00240398	0.401753
		50	0.3578	0.00157674	0.00158801	0.00229017	0.401759
		100	0.7156	0.00156462	0.00157585	0.00225445	0.401737
	5	20	0.1431	0.00161414	0.00162590	0.00240398	0.401754
		50	0.3578	0.00157675	0.00158821	0.00229017	0.401745
		100	0.7156	0.00156462	0.00157583	0.00225445	0.401726
10^5	1	20	0.04526	0.000512618	0.000513737	0.000767001	0.401741
		50	0.1131	0.000500332	0.000501449	0.000729712	0.401809
		100	0.2263	0.000496672	0.000497830	0.000718483	0.401737
	5	20	0.04526	0.000512618	0.000513854	0.000767001	0.401772
		50	0.1131	0.000499062	0.000500277	0.000727769	0.401806
		100	0.2263	0.000496672	0.000497795	0.000718483	0.401745
10^6	1	20	0.01431	0.000162288	0.000162393	0.000243341	0.401835
		50	0.03578	0.000158479	0.000158585	0.000231440	0.401862
		100	0.07156	0.000157686	0.000157808	0.000228397	0.401548
	5	20	0.01431	0.000162288	0.000162435	0.000243187	0.401752
		50	0.03578	0.000158479	0.000158598	0.00023144	0.401711
		100	0.07156	0.000157686	0.000157797	0.000228397	0.401461
10^7	1	20	0.004526	$5.13502 \cdot 10^{-5}$	$5.13615 \cdot 10^{-5}$	$7.69844 \cdot 10^{-5}$	0.401964
		50	0.01131	$5.01145 \cdot 10^{-5}$	$5.01246 \cdot 10^{-5}$	$7.32173 \cdot 10^{-5}$	0.401900
		100	0.02263	$4.97464 \cdot 10^{-5}$	$4.97587 \cdot 10^{-5}$	$7.20836 \cdot 10^{-5}$	0.401777
	5	20	0.004526	$5.13502 \cdot 10^{-5}$	$5.13626 \cdot 10^{-5}$	$7.69844 \cdot 10^{-5}$	0.401812
		50	0.01131	$5.01145 \cdot 10^{-5}$	$5.01245 \cdot 10^{-5}$	$7.32173 \cdot 10^{-5}$	0.401969
		100	0.02263	$4.97464 \cdot 10^{-5}$	$4.97569 \cdot 10^{-5}$	$7.20836 \cdot 10^{-5}$	0.401686

Моделирование стеганосистемы с разнесением по времени для звукового покрывающего сообщения

Используется музыкальный аудиофайл в формате WAV с частотой дискретизации 44100 Гц длительностью около 29 секунд. Отношение ПС/шум η_c выбрано 10 дБ, в то время как отношение ЦВЗ/шум η_W^{-1} выбрано 20 дБ. Используется правило погружения (9), причем $P_0 = 0.1$. Зависимость интенсивности I аудио-сигнала от времени t представлена на рис. 2, где стрелками показаны отсчеты с внедрением. На основе сравнительного анализа видно, что шум слегка искажает аудиосигнал, также это заметно на слух, в то время как результат процедуры внедрения не заметен.

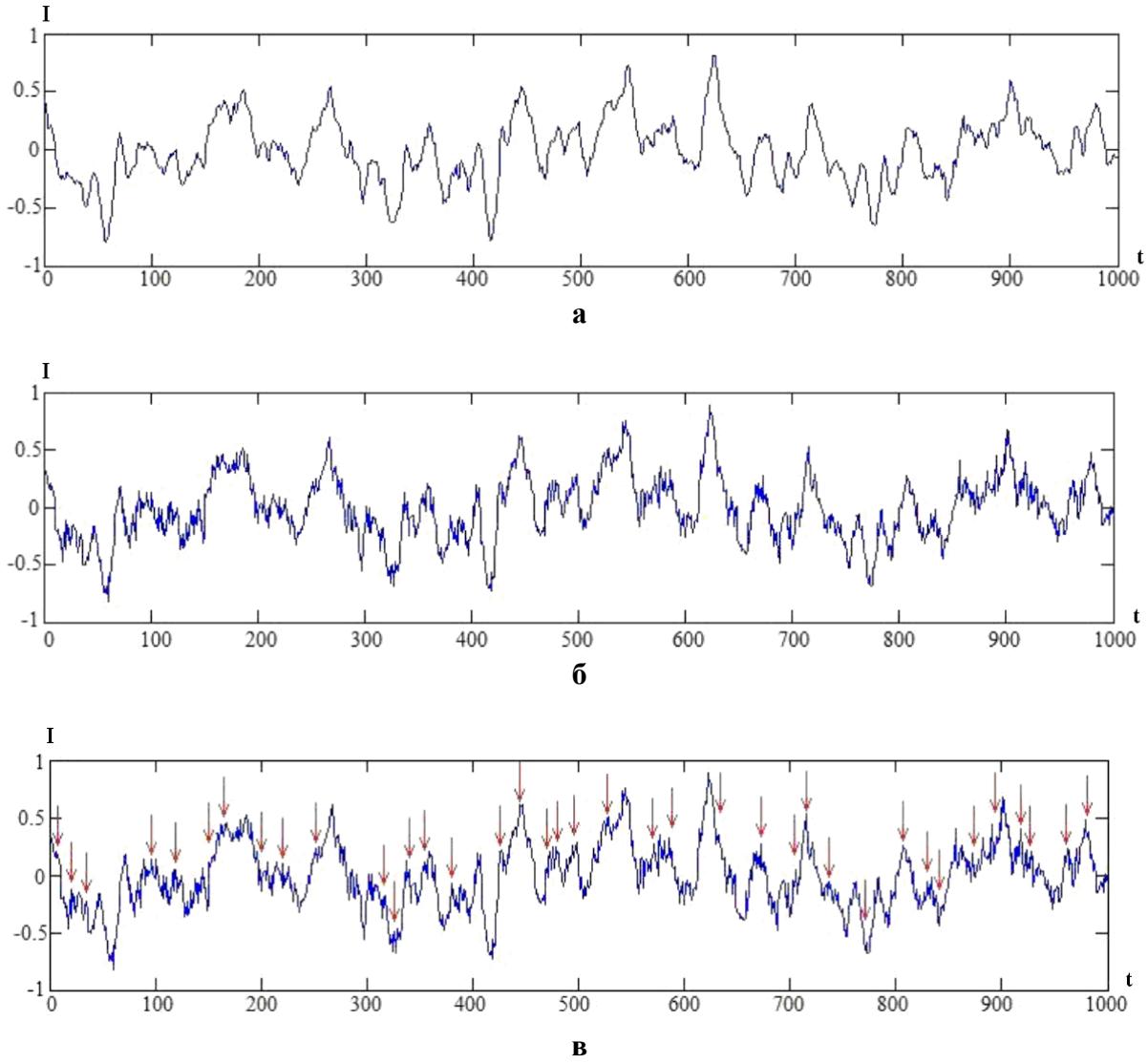

Рис. 2. Синограммы тестового аудиофайла: а – исходного; б –после прохождения по зашумленному каналу; в – после внедрения скрытого сообщения

На рис. 3 показаны синограммы шума в канале до и после внедрения стегано-сигнала. Конечно незаметность внедрения стегосигнала на слух, также как и на глаз, никоим образом не доказывает невозможность его обнаружить статистическим методом. Факт невозможности обнаружения лучшим статистическим методом был доказан в предыдущем разделе.

В табл. 3 представлены результаты симуляции вероятности ошибки $P_{ош}$ в зависимости от длины блока N_0 и отношения η_W, вероятность ошибки $\widetilde{P}_{ош}$, рассчитанная в соответствии с (7). Из таблицы видно, что защищенность СРВ, полученная в результате симуляции, показывает лучшие результаты, чем теоретическая ожидаемая граница.

Таблица 3.

Результаты вычислений вероятности ошибки $P_{ош}$, полученной после декодирования по правилу (6) и теоретической вероятности ошибки $\widetilde{P}_{ош}$, вычисленной в (7) при $N = N_0$, для разных значений параметров η_W и N_0

η_W	N_0	$P_{ош}$	$\widetilde{P}_{ош}$
20	210	5.0×10^{-4}	0.001
50	496	6.0×10^{-4}	0.001
100	973	5.5×10^{-4}	0.001

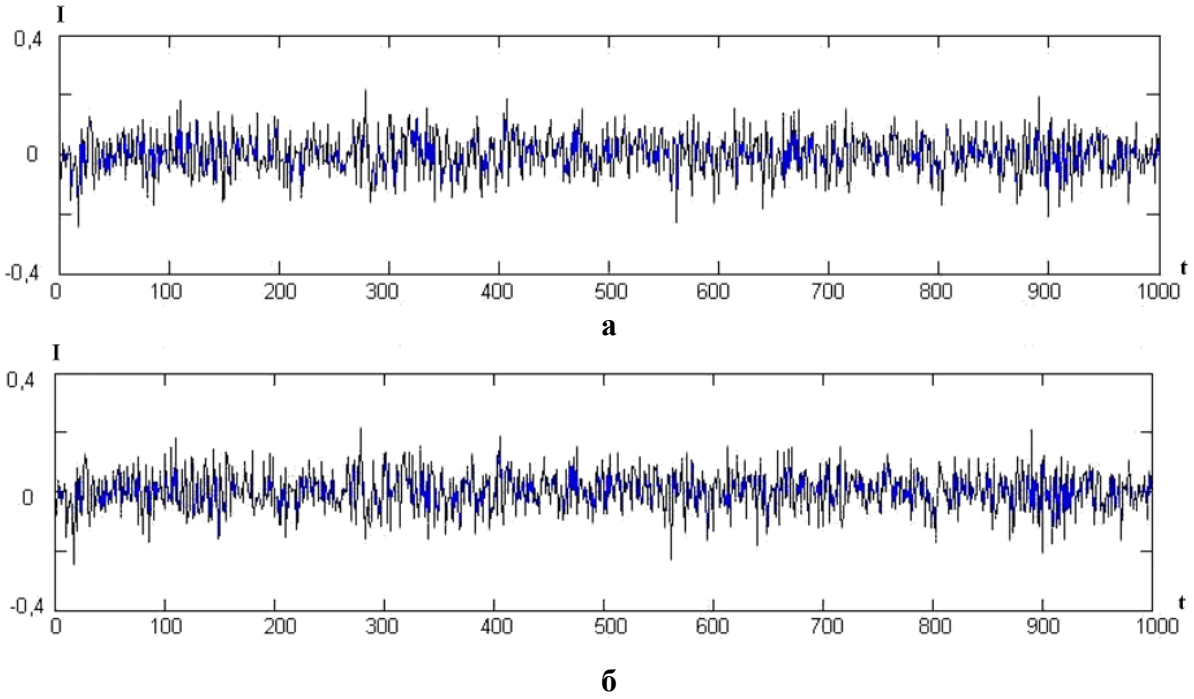

Рис. 3. Синограммы шума в канале: a – до внедрения скрытого сообщения; b –после внедрения скрытого сообщения по правилу (9)

Выводы

В данной работе представлена стеганографическая система для зашумленного канала – стеганографическая система с разнесением по времени, способная обеспечить необходимые уровни секретности и надежности восприятия сокрытого сообщения при реализуемом на практике значении отношения сигнал/шум. Доказано, что секретность и надежность восприятия такой системы могут быть обеспечены одновременно при правильном выборе ее параметров. Основным недостатком предложенной системы является низкая скорость внедрения, которая влечет за собой увеличение времени формирования стегосигнала одновременно с ограничением объема скрытой информации. Коды коррекции ошибок способны улучшить эту ситуацию, но лишь незначи-

тельно. Тем не менее, это свойство является своеобразной платой за невозможность обнаружения внедренного сообщения, даже при условии, что атакующая сторона обладает знанием покрывающего сообщения.

Также показано, что субоптимальное детектирование стеганосистемы (16) практически настолько же эффективно, как и оптимальное (основанное на отношении максимального подобия). Симуляция СРВ с использованием в качестве ПС аудиофайла показывает, что обнаружение внедренной информации на слух или на глаз невозможно, при том, что внедренные биты могут быть уверенно извлечены.

В дальнейшем представляется интересным продолжить исследование СРВ для ПС в цифровом формате, а также методы извлечения стеганосообщения при использовании неинформированного декодера, т.е. при неизвестном ПС на приемной части. Это возможно, например, на основе применения методов, рассмотренных в [6].

Список литературы

1. Korjik V.I., Lee M.H., Morales-Luna G. Stegosystems based on noisy channels // Proceeding of IX Spanish Meeting on Cryptology and Information Security. – Barcelona: Universidad Autonoma de Barcelona, 2006. – PP. 379-387.
2. Иванов В.А. Об искусственном зашумлении каналов передачи данных // Труды по дискретной математике. – 2004. – Том 8. – С. 99-115.
3. Cachin C. An information-theoretic model for steganography / C. Cachin // Proceeding of 2nd Workshop on Information Hiding, Lecture Notes in Computer Science. – USA: Springer, 1998. – Vol.1525. – PP. 306-318.
4. Van der Waerden B.L. Mathematische Statistik. – Berlin: Springer-Verlag, 1957; English transl. of 2nd (1965) ed. Springer-Verlag, Berlin and New York, 1969. – 367 p.
5. MacWilliams F.J. The Theory of Error-Correcting Codes / F.J. MacWilliams, N.J.A. Sloane. – Ney York : North Holland Publishing Co., 1977. – 762 p.
6. Malvar H.S. Improved spread spectrum: A new modulation technique for robust watermarking / H.S. Malvar, D.A.F. Florencio // IEEE Transaction on Signal Processing. – 2001. – Vol.51, Iss.4. – PP. 898-905.

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРИХОВУВАННЯ ІНФОРМАЦІЇ ДЛЯ СИСТЕМ З ЗАШУМЛЕННИМИ КАНАЛАМИ ЗВ'ЯЗКУ

І.І. Маракова[1], О.О. Яковенко[2]

[1] Telecom Bretagne,
Technopôle Brest-Iroise, CS 83818, 29238 Brest Cedex 3, France; e-mail: marakova.irina@gmail.com
[2] Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна: e-mail: iakovenko.oleksandr@gmail.com

Розглядається система передачі прихованої інформації по зашумленних каналах зв'язку і сценарій, при якому атакуюча сторона не має іншого доступу до стеганосигналу, окрім як в ґаусовому каналі. При такому підході потрібно забезпечити практично недосяжну на практиці величину відношення сигнал/шум, особливо з урахуванням того, що покриваюче повідомлення може бути відомо стороні, що атакує. Для вирішення цієї проблеми запропоновано використовувати стеганосистему з рознесенням за часом (СРЧ). Доведена можливість побудови СРЧ із заданим рівнем секретності і надійності сприйняття прихованого сигналу. Розглянуто питання оптимізації параметрів на основі використання кодів корекції помилок. Представлені результати моделювання за допомогою реалізації СРЧ для покриваючих повідомлень у вигляді цифрових звукових файлів формату WAV.
Ключові слова: стеганосистема, покриваюче повідомлення, коди корекції помилок, ґаусовий канал з шумами, відносна ентропія

INFORMATION HIDING EFFICIENCY IMPROVEMENT FOR NOISY CHANNEL COMMUNICATION SYSTEMS

Irina I. Marakova[1], Alexander A. Iakovenko[2]

[1] Telecom Bretagne,
Technopôle Brest-Iroise, CS 83818, 29238 Brest Cedex 3, France; e-mail: marakova.irina@gmail.com
[2] Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: iakovenko.oleksandr@gmail.com

A system of hidden information transmission through a noisy communication channels, and a scenario where an attacker has no other access to steganographic signal, except in the Gaussian channel, are considered. With such an approach, it is required to provide virtually unattainable in practice magnitude of the signal/noise ratio, especially considering the fact that the covering message may be known to attackers. The steganographic systems with time spread (STS) are offered to solve this problem. STS constructions with a given level of privacy and perception fidelity are proved possible. The means of parameter optimization using error correcting codes is also considered. Results of simulation for STS over a WAV digital audio file format are presented.
Keywords: steganographic systems, covering message, error correction codes, Gaussian channel with noise, relative entropy

УДК 004.056.5:518

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 1, pp. 18-27

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ УСТОЙЧИВОСТИ СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА К АТАКЕ СЖАТИЕМ

А.А. Кобозева

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

На основе общего подхода к анализу состояния и технологии функционирования информационных систем, разработанного автором ранее, предлагается новый подход к решению проблемы устойчивости стеганографических алгоритмов к атаке сжатием. В работе получены формальные достаточные условия малой чувствительности стеганосообщения к сжатию с одновременным обеспечением его надежности восприятия. Предложенный подход позволит автоматизировать процесс анализа существующих или разрабатываемых стеганографических алгоритмов с точки зрения их устойчивости к сжатию путем оценки возмущений сингулярных чисел матрицы (матриц) контейнера, произошедших в процессе стеганопреобразования, а также даст возможность априорного выбора из множества стеганосообщений наименее чувствительного к сжатию.

Ключевые слова: стеганографический алгоритм, атака сжатием, сингулярные числа

Введение

Надежная защита информации, которая в настоящее время все больше становится товаром, причем одним из наиболее дорогих [1], от несанкционированного доступа является актуальной, но не решенной в полном объеме проблемой. Одно из перспективных направлений защиты информации сформировали современные методы стеганографии [2-6], особенностью которых является то, что скрываемое сообщение, или дополнительная информация (ДИ), встраивается в некоторый объект, не привлекающий внимание, или контейнер, который затем открыто пересылается адресату по каналу связи или хранится в таком виде.

В последнее время создано много методов сокрытия информации в разных типах и форматах данных [4, 7-9], и сейчас этот процесс активно развивается, поскольку, хотя современные компьютерные технологии обработки данных дали возможность широкого использования криптографических методов защиты информации, для ряда прикладных задач информационной безопасности криптографических методов недостаточно [7].

Процесс погружения ДИ в контейнер, или основное сообщение (ОС), будем называть стеганопреобразованием (СП), а результат СП – стеганосообщением (СС). Для определенности везде ниже как ОС используется монохромное цифровое изображение (ЦИ), а как ДИ – сформированная случайным образом бинарная последовательность.

К любому стеганографическому алгоритму (СА) выдвигается ряд требований, среди которых важную роль играет требование устойчивости к преднамеренным (непреднамеренным) атакам [2, 7, 8]. Согласно [4], СА назовем устойчивым (неустойчивым), если сформированное им СС является нечувствительным (чувствительным) к возмущающим воздействиям.

Созданию устойчивых алгоритмов в современной печати уделено достаточно внимания, однако вопрос создания СА, устойчивых к атаке сжатием, которая является чрезвычайно распространенной благодаря популярности использования форматов с потерями для хранения и передачи цифровых сигналов (в частности ЦИ), остается актуальным и на сегодняшний день. Как правило, все существующие СА такого плана осуществляют погружение ДИ в частотной области контейнера и, при условии обеспечения надежности восприятия СС, выдерживают лишь незначительное сжатие [2, 3, 10, 11]. И хотя в некоторых работах, как, например, в [11], декларируется достижение устойчивости предлагаемого алгоритма к сжатию для любого коэффициента качества, представленные теоретические обоснования и результаты тестирования его работы на 10 ЦИ выглядят неубедительно.

Поскольку атака сжатием на СС является одним из видов возмущающих воздействий, сравнение устойчивости различных СА к атаке сжатием можно проводить, сравнивая чувствительность к возмущающим воздействиям формируемых ими СС, используя подход, предложенный автором ранее в [12], основанный на теории возмущений и матричном анализе. Сложность в использовании данного подхода заключается в том, что он носит преимущественно качественный характер. Его развитием стали последующие работы, в частности, [13], результатом которых явилось создание метода количественной оценки устойчивости СА к произвольным возмущающим воздействиям, основой которого является оценка объема защищенной информации в СС, проводимая с учетом возмущений сингулярных векторов (СНВ) соответствующих матриц ОС при СП. Геометрическая интерпретация процесса СП дана на рис. 1, где $u_i, i=\overline{1,3}$, – СНВ матрицы (подматрицы) ОС, а $\overline{u}_i, i=\overline{1,3}$, – СНВ СС. Однако предложенный подход является «слишком универсальным», он не учитывает особенностей конкретного возмущающего воздействия – сжатия. Кроме того, оценка чувствительности СС через оценку чувствительности возмущенных в ходе СП СНВ вызывает затруднение, поскольку чувствительность СНВ одной и той же матрицы различна и зависит от отделенностей соответствующих сингулярных чисел (СНЧ) [4, 13]. Более предпочтительным и желаемым является сведение оценки устойчивости СА к локализации возмущений только СНЧ, произошедших в ходе СП, в силу их хорошей обусловленности [14].

Таким образом, актуальным остается поиск новых путей и подходов к принципиальному решению проблемы обеспечения для разрабатываемых СА устойчивости к сжатию, которую далее будем называть проблемой сжатия (ПС).

Цель исследования и постановка задачи

В [14] на основе теории возмущений и матричного анализа был разработан общий подход к анализу состояния и технологии функционирования информационных систем (ОПАИС), в частности, систем защиты информации, основная идея которого заключается в следующем.

Произвольная информационная система, в том числе, стеганографическая система (или отдельно рассматриваемый контейнер, СС), формализуется в виде двумерной матрицы (конечного множества двумерных матриц), что позволяет свести анализ состояния системы к анализу свойств соответствующих матриц. Для простоты изложения, не ограничивая при этом общности рассуждений, в качестве математической модели произвольной информационной системы рассматривается двумерная $m \times n$-матрица F. Результат любых действий, производимых над системой, в общем случае можно представить как возмущение ΔF матрицы F, сами действия – возмущающие воздействия на F, а задача любого преобразования системы, т.е. генерации новой, для которой старая является исходными данными, – это задача получения возмущенной

матрицы для исходной матрицы F, причем результирующая матрица очевидно удовлетворяет соотношению: $\overline{F} = F + \Delta F$, где $\Delta F = f(F)$, т.е. ΔF является некоторой функцией матрицы F. Таким образом, в качестве набора формальных параметров, однозначно определяющих и всесторонне характеризующих информационную систему, можно использовать любой из наборов, который однозначно определяет произвольную двумерную матрицу – полных наборов параметров [15]. Одним из таких наборов, преимущества которого подробно обсуждаются в [14], является совокупность СНЧ и СНВ, полученных при помощи нормального спектрального разложения матрицы, отвечающей рассматриваемой системе.

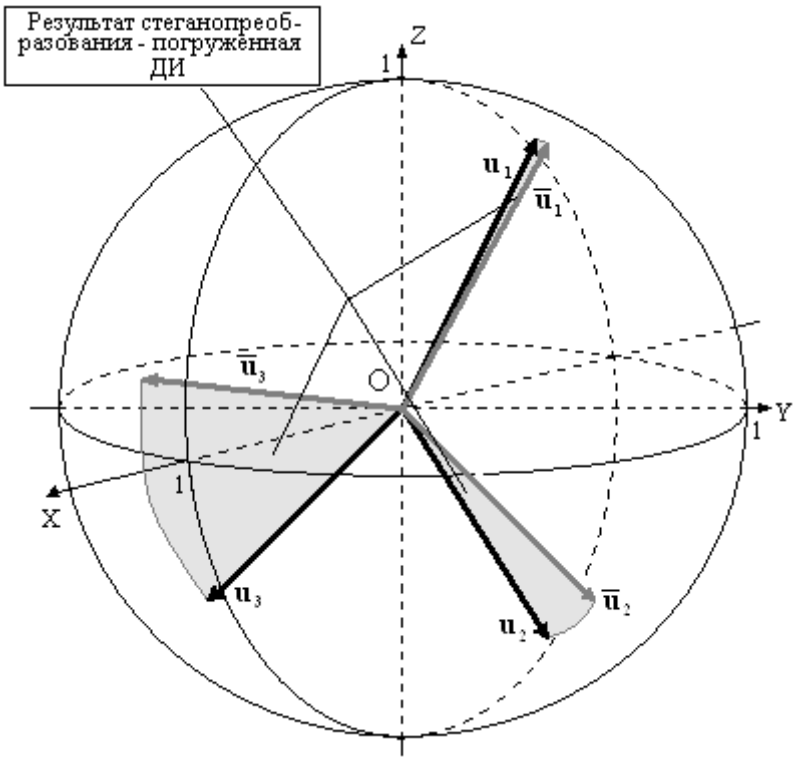

Рис. 1. Формальное представление результата стеганопреобразования

Любое преобразование информационной системы возмутит ее матрицу F, следовательно определенным образом возмутит ее СНЧ и СНВ, а значит любое преобразование, в том числе и СП, представимо в виде совокупности возмущений СНЧ и (или) СНВ соответствующей матрицы (матриц). Это позволяет естественным образом свести задачу анализа процесса стеганопреобразования к анализу возмущений СНЧ и СНВ соответствующей матрицы (матриц) контейнера (СС), независимо от рассматриваемой области сигнала, конкретики используемого СА или предпринятой атаки [4].

Таким образом, о результате преобразования информационной системы (в частности, стеганосистемы), ее свойствах, характеристиках можно судить по характерным особенностям совокупности возмущений однозначно определяющих ее параметров – СНЧ и СНВ соответствующей матрицы (матриц). Это утверждение является краеугольным камнем для разработок, предложенных в настоящей работе.

Целью работы является получение достаточных условий обеспечения устойчивости СА к атаке сжатием с одновременным обеспечением надежности восприятия формируемого СС путем разработки принципиально нового общего подхода к решению ПС на основе адаптации ОПАИС в область стеганографии, что даст возможность автоматизировать процесс анализа существующих или разрабатываемых

СА с точки зрения их устойчивости к сжатию и формально определить необходимые корректировки СА в случае его неустойчивости.

Для достижения поставленной цели необходимо решить следующие *задачи*:

1) Выделить из совокупности формальных параметров, определяющих результат СП, – СНЧ (СНВ) соответствующих матриц, отвечающих ОС, наименее чувствительные к операции сжатия;

2) Получить формальное представление процесса сжатия в виде совокупности определенных возмущений СНЧ (СНВ) матриц ЦИ.

Основная часть

Конкретизируем понятие СА, устойчивого к атаке сжатием.

Общая схема сжатия (с потерями) для ЦИ, которая использована в наиболее распространенных на сегодня стандартах, в частности, в стандарте JPEG, состоит из трех основных шагов:

- отображение в частотную область после предварительного стандартного разбиения матрицы изображения на 8×8-блоки;
- квантование полученных частотных коэффициентов;
- энтропийное кодирование.

Восстановление включает в себя шаги, обратные к перечисленным выше, в обратном порядке [15].

Независимо от конкретики непосредственной реализации сжатия отметим, что в силу специфики человеческого зрения сжатие происходит таким образом, что его результат приводит к исключению из сигнала его высокочастотных (а возможно, и среднечастотных) составляющих за счет обнуления соответствующих коэффициентов. В силу этого для определенности изложения, никак не ограничивая общности рассуждений, везде ниже атака сжатием, направленная на СС, моделируется путем сохранения этого СС в одном из наиболее распространенных на сегодняшний день форматов – формате JPEG с потерями, основанном на дискретном косинусном преобразовании.

В силу специфики предметной области решаемой задачи не имеет смысла рассматривать сжатие с потенциально произвольным коэффициентом, поскольку после проведенной на СС атаки надежность восприятия этого СС не должна быть нарушена [2].

Учитывая [16], в данной работе рассматриваются варианты JPEG-сжатия ЦИ, которое осуществляется в среде *Adobe* Photoshop с коэффициентами качества $Q\in\{8,9,10,11,12\}$ (для меньших значений Q надежность восприятия, устанавливаемая путем субъективного ранжирования, может нарушаться). Эффективность декодирования СА оценивается величиной объема восстановленной информации (ОВИ), который вычисляется согласно формуле

$$\frac{k-\sum_{i=1}^{k} p_i \oplus \overline{p}_i}{k}\cdot 100\%,$$

где

$p_1, p_2, ..., p_k$, $p_i\in\{0,1\}$, $i=1,...,k$, – последовательность, которая отвечает встраиваемому секретному сообщению;

$\overline{p}_1, \overline{p}_2, ..., \overline{p}_k$, $\overline{p}_i\in\{0,1\}$, $i=1,...,k$, – декодированное из СС секретное сообщение;

$\oplus$ – операция логического исключающего ИЛИ.

Поскольку до настоящего момента нигде в открытой печати не была установлена однозначная точная нижняя граница величины, каким-либо образом характеризующей эффективность декодирования СА, для которой алгоритм можно называть устойчивым к операции сжатия (чаще всего такая оценка носит не количественный, а качественный характер), условимся считать СА *устойчивым* к сжатию, если ОВИ после атаки на СС с $Q \in \{8,9,10,11,12\}$, окажется не меньше 75% для $Q = 8$. ОВИ является численной оценкой устойчивости СА.

Последний шаг восстановления ЦИ после сжатия возвращает его из частотной в пространственную область. При этом коэффициенты получаемой матрицы будут иметь вещественные значения, которые могут выходить за границы множества $[0,255]$. Результат восстановления на этой стадии назовем частичным (ЧВ). Окончательное, или полное, восстановление (ПВ) ЦИ будет получено после округления значений яркости до целых и введения их в границы 0...255.

Процесс квантования приводит к обнулению коэффициентов, отвечающих, как правило, высоким частотам сигнала, за счет чего и происходит сжатие. Но при достаточно большом коэффициенте сжатия возможно обнуление и среднечастотных коэффициентов, поэтому использование для погружения ДИ средней части частотного спектра, о чем говорилось выше, формирует СС, которое принципиально может выдерживать лишь незначительное сжатие.

Пусть F – $m \times n$-матрица контейнера. Для F существует нормальное сингулярное разложение [14]: $F = U\Sigma V^T$, где U, V – ортогональные матрицы размера $m \times n$ и $n \times n$ соответственно, столбцы $u_1,...,u_n$ матрицы U, называемые левыми СНВ, лексикографически положительны [14] (столбцы $v_1,...,v_n$ матрицы V называют правыми СНВ матрицы F); $\Sigma = diag(\sigma_1,...,\sigma_n)$, $\sigma_1 \geq ... \geq \sigma_n \geq 0$ – сингулярные числа (СНЧ); (σ_i, u_i, v_i) называется сингулярной тройкой F. В [14] показано, что невырожденная матрица имеет единственное нормальное сингулярное разложение, если ее СНЧ попарно различны, которое может представляться в форме внешних произведений: $F = \sum_{k=1}^{n} \sigma_k u_k v_k^T$. Матрицу

$$S_k = \sigma_k u_k v_k^T \qquad (1)$$

в соответствии с [17] назовем *k*-й составляющей изображения F.

В [17] в результате представительного вычислительного эксперимента было установлено: *k*-ые составляющие (1) изображения, отвечающие сингулярным тройкам с максимальными СНЧ, соответствуют, главным образом, низкочастотным составляющим сигнала; *k*-ые составляющие ЦИ, отвечающие тройкам с минимальными (средними по величине) СНЧ, несут в себе, в основном, высокочастотные (среднечастотные) составляющие.

Результат сжатия в соответствии с [15] – это обнуление коэффициентов при высоких (и возможно средних) частотных составляющих в частотной области ЦИ. При использовании ОПАИС сжатие, как и любое другое возмущающее воздействие, формально представимо в виде возмущения сингулярных троек, главным результатом которого является обнуление наименьших (и возможно средних) по величине СНЧ, что приведет к удалению из F *k*-х составляющих (1), где k имеет значения равные или близкие к n (вплоть до сравнимых с $n/2$), что подтверждается результатами вычислительного эксперимента [18]. Таким образом, получено решение задачи 2.

Наибольшее СНЧ практически не возмущаются в процессе сжатия. Это не случайно. Сингулярные тройки, отвечающие максимальным СНЧ, соответствуют,

главным образом, низкочастотным составляющим сигнала, а значит являются наименее чувствительными к сжатию, что принципиально решает задачу 1.

Любое СП в соответствии с ОПАИС определяется совокупностью возмущений СНЧ (СНВ) матрицы контейнера F (или ее подматриц). Учитывая, что рассматриваемая в работе задача связана с процессом сжатия, осуществление которого предполагает предварительное разбиение матрицы ЦИ на 8×8-блоки, результат СП формализуем в виде совокупностей возмущений СНЧ (СНВ) блоков [4]. Для достижения цели работы необходимо выделить из СНЧ (СНВ) 8×8-блоков такие, возмущения которых в ходе СП обеспечат нечувствительность получаемого в результате СС к конкретному возмущающему воздействию – сжатию. В соответствии с полученным выше решением задачи 1 результатом СП без учета визуальных искажений, происходящих в СС, должно быть возмущение наибольших СНЧ. Однако, изменение величины максимального СНЧ в блоках всего на 5-8%, возмущение которого в ходе СП очевидно является наиболее желаемым, как показывает вычислительный эксперимент, приводит к появлению явных артефактов на ЦИ. Такой же порядок относительного изменения второго по величине СНЧ, как правило, не приводит к нарушению надежности восприятия СС [4] (рис. 2).

а **б**

в

Рис. 2. Результат возмущения СНЧ блоков матрицы ЦИ: а – исходное ЦИ; б – возмущению подвергнуто максимальное СНЧ блока; в – возмущению подвергнуто второе по величине СНЧ блока

Таким образом, имеет место следующее утверждение.

Утверждение. Для обеспечения устойчивости СА к сжатию с одновременным обеспечением большой вероятности надежности восприятия формируемого СС

достаточно производить погружение ДИ таким образом, чтобы формальным результатом СП было возмущение второго (и возможно третьего) по значению СНЧ в сингулярных спектрах блоков матрицы контейнера, полученных после ее стандартного разбиения. Если же СП формально выразится в возмущении средних и наименьших по значению СНЧ, то (при большой вероятности обеспечения надежности восприятия СС) такой СА окажется неустойчивым к сжатию.

Замечание 1. Как правило, результат СП существующих СА представляется в виде возмущения практически всех СНЧ соответствующей матрицы (матриц): ДИ «распределяется» по всем составляющим сингулярного спектра. Такая картина будет наблюдаться, если процесс СП не сводится к непосредственному возмущению конкретных СНЧ, как, например, в [19]. При сравнении потенциальной устойчивости различных СА к возможной атаке сжатием предпочтение следует отдать тому, который в ходе СП более остальных СА возмутит максимальные СНЧ.

Для практического подтверждения истинности сформулированного утверждения был рассмотрен один из наиболее широко распространенных СА, который считается устойчивым к атаке сжатием и часто используется для сравнения с подобными вновь создаваемыми или модифицируемыми алгоритмами [10, 11], – метод Коха (E. Koch) и Жао (J. Zhao) (МКЖ) [3]. МКЖ производит внедрение в коэффициенты дискретного косинусного преобразования (ДКП) средней части частотного спектра 8×8-блоков путем их взаимного изменения. Коэффициенты ДКП, выбранные для внедрения ДИ, задаются своими координатами в 8×8-массиве – $(i_1, j_1), (i_2, j_2)$ (рекомендуемые в [3] для внедрения ДИ коэффициенты (5,4) и (4,5)). Вычислительный эксперимент, в котором участвовало более 200 ЦИ в формате TIF, проводился в среде *MathWorks* MATLAB. После СП полученное СС сохранялось в *Adobe* Photoshop с $Q = 8,9,10,11,12$. Результаты эксперимента представлены в табл. 1.

Таблица 1.

Результаты декодирования секретной информации в методе Коха и Жао

$(i_1, j_1), (i_2, j_2)$	Q	ОВИ (%)	Обеспечение надежности восприятия СС
(5,4), (4,5)	8	54.6339	+
	9	91.7782	+
	10	99.1146	+
	11	99.9362	+
	12	99.9947	+
(3,4), (4,3)	8	71.3798	+
	9	94.9230	+
	10	99.0976	+
	11	99.9126	+
	12	99.9782	+
(2,3), (3,2)	8	98.0660	-
	9	99.7319	-
	10	99.8848	-
	11	99.9132	-
	12	99.9392	-

Проанализируем результаты СП, произведенного МКЖ, с точки зрения их представления в виде совокупности возмущений СНЧ блоков матрицы контейнера и соответствия их сформулированному выше утверждению. В табл. 2 для примера

приведены типичные результаты для одного и того же блока тестируемого ЦИ. Эти результаты полностью соответствуют утверждению. Так МКЖ, использующий для СП коэффициенты ДКП с индексами (4,5) и (5,4) принципиально не мог оказаться устойчивым к сжатию с малым коэффициентом качества, что и было получено ранее при тестировании его работы (табл. 1), т.к. такое СП практически не возмутило наибольшие СНЧ. В соответствии с результатами табл. 2 и утверждением, устойчивым к сжатию должен оказаться МКЖ, использующий коэффициенты ДКП с индексами (2,3) и (3,2), что полностью отвечает результатам его работы на практике (табл. 1) (хотя такой вариант МКЖ не обеспечивает надежность восприятия, а значит является неприемлемым).

Таблица 2.

Возмущения СНЧ блока ЦИ, хранимого в формате TIF, при СП методом Коха и Жао (СС после СП сохраняется без потерь)

$(i_1, j_1), (i_2, j_2)$	Характер восстановления ЦИ при обратном ДКП	Относительные погрешности СНЧ в порядке, отвечающем $\sigma_1, \sigma_2, ..., \sigma_8$ (%)
(5,4), (4,5)	ЧВ	0.0000, 0.0899, 3.7185, 32.0837, 93.2585, 0.0623, 265.5867, 82.1709
	ПВ	0.0000, 0.0362, 3.3645, 27.8843, 97.7085, 0.0402, 258.8111, 93.8611
(3,4), (4,3)	ЧВ	0.0000, 0.3338, 14.9730, 0.5167, 17.2428, 3.2857, 125.4383, 62.1174
	ПВ	0.0000, 0.4575, 14.7477, 0.4936, 11.3472, 1.9157, 148.5082, 62.6708
(2,3), (3,2)	ЧВ	0.0013, 11.4289, 3.2428, 1.3678, 8.1935, 12.7950, 0.2274, 24.0782
	ПВ	0.0013, 11.4957, 2.8944, 1.5089, 2.2150, 13.7399, 7.9410, 25.0259

Заключение

В работе предложен новый подход к решению проблемы обеспечения СА устойчивости к атаке сжатием при его разработке, основанный на ОПАИС, в соответствии с которым любое возмущающее воздействие, направленное на ОС, в частности СП, а также возмущение СС, в частности, его сжатие, рассматривается как возмущение соответствующей матрицы (матриц) контейнера (СС).

Разработанный подход:

- позволил получить достаточное условие обеспечения устойчивости СА к сжатию с одновременным обеспечением большой вероятности надежности восприятия формируемого СС, которое никак не зависит от используемой для погружения ДИ области контейнера (пространственной или частотной) и конкретики СА, и определяется лишь локализацией и относительной величиной возмущений СНЧ соответствующих матриц ОС, произошедших в ходе СП;
- дал возможность для проведения выбора СС, наименее чувствительного к сжатию: чем большему возмущению в процесс СП подверглись максимальные СНЧ блоков матрицы контейнера, тем менее чувствительно к сжатию полученное СС;
- позволит автоматизировать процесс анализа существующих или разрабатываемых СА с точки зрения их устойчивости к сжатию путем оценки

возмущений различных СНЧ в процессе СП: если СП формально выразится в возмущении максимальных (средних и наименьших) по значению СНЧ блоков матрицы ОС, то соответствующий СА будет устойчивым (неустойчивым) к сжатию.

Список литературы

1. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – К. : Юниор, 2003. – 501 с.
2. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М. : Солон-Пресс, 2002. – 272 с.
3. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К. : МК-Пресс, 2006. – 249 с.
4. Кобозєва А.А. Аналіз захищеності інформаційних систем / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко. – К. : Вид. ДУІКТ, 2010. – 316 с.
5. Böhme R. Advanced Statistical Steganalysis. – Berlin: Springer-Verlag, 2010. – 300 p.
6. Ленков С.В. Методы и средства защиты информации [Текст]: в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К.: Арий, 2008. – . –
Т.2: Информационная безопасность. – 2008. – 344 с.
7. Корольов В.Ю. Планування досліджень методів стеганографії та стеганоаналізу / В.Ю. Корольов, В.В. Поліновський, В.А. Герасименко, М.Л. Горінштейн // Вісник Хмельницького національного університету. Технічні науки. – 2011. – №4. – С. 187-196.
8. Королев В.Ю. Стеганография по методу наименее значимого бита на базе персонализированных флеш-накопителей / В.Ю. Королев, В.В. Полиновский, В.А. Герасименко // Управляющие системы и машины. – 2011. – №1(231). – С. 79-87.
9. 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.
10. 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.
11. Михайличенко О.В. Алгоритм встраивания цифровых водяных знаков в единичный коэффициент матрицы дискретно-косинусного преобразования / О.В. Михайличенко, Н.Н. Прохожев // Сборник трудов VI Всероссийской конференции молодых ученых. Выпуск 6. Информационные технологии. – СПб. : СПбГУ ИТМО, 2009. – С. 644-648.
12. Кобозєва А.А. Загальний підхід до оцінки властивостей стеганографічного алгоритму, заснований на теорії збурень / Інформаційні технології та комп'ютерна інженерія. – 2008. – №1(11). – С. 164-171.
13. Кобозева А.А. Оценка чувствительности стегосообщения к возмущающим воздействиям / А.А. Кобозева, Е.В. Нариманова // Системні дослідження та інформаційні технології. – 2008. – №3. – С. 52-65.
14. Кобозева А.А. Анализ информационной безопасности / А.А. Кобозева, В.А. Хорошко. – К. : Изд. ГУИКТ, 2009. – 251 с.
15. Гонсалес Р. Цифровая обработка изображений [Текст] : пер. с англ. / Р.С. Гонсалес, Р.Э. Вудс ; ред. пер. ЧоП. А. Чочиа. – М. : Техносфера, 2006. – 1070 с.
16. Кобозева А.А. Метод выявления результатов размытия цифрового изображения / А.А. Кобозева, В.В. Зорило // Сучасна спеціальна техніка. – 2010. – №3(22). – С. 52-63.
17. Кобозева А.А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации / А.А. Кобозева // Искусственный интеллект. – 2007. – №4. – С. 531-538.
18. Кобозева А.А. Учет свойств нормального спектрального разложения матрицы контейнера при обеспечении надежности восприятия стегосообщения / А.А. Кобозева, Е.А. Трифонова // Вестник Национального технического университета «Харьковский политехнический институт»: Сборник научных трудов. Тематический выпуск «Системный анализ, управление и информационные технологии». – 2007. – №18. – С. 81-93.
19. Кобозева А.А. Стеганографический метод, основанный на преобразовании спектра симметричной матрицы / А.А. Кобозева // Праці УНДІРТ. – 2006. – №4(48). – С. 44-52.

ПРОБЛЕМА ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ СТЕГАНОГРАФІЧНОГО АЛГОРИТМУ ДО АТАК СТИСКОМ

А.А. Кобозєва

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

На основі загального підходу до аналізу стану й технології функціонування інформаційних систем, розробленого автором раніше, пропонується новий підхід до рішення проблеми стійкості стеганографічних алгоритмів до атаки стиском. В роботі отримані формальні достатні умови малої чутливості стеганоповідомлення до стиску з одночасним забезпеченням його надійності сприйняття. Запропонований підхід дозволить автоматизувати процес аналізу існуючих або розроблювальних стеганографічних алгоритмів з погляду їхньої стійкості до стиску шляхом оцінки збурень сингулярних чисел матриці (матриць) контейнера, що відбулися в процесі стеганоперетворення, а також дасть можливість апріорного вибору з множини стеганоповідомлень найменш чутливого до стиску.
Ключові слова: стеганографічний алгоритм, атака стиском, сингулярні числа

THE PROBLEM OF STEGANOGRAPHIC ALGORITHM STABILITY TO THE COMPRESSION ATTACKS

Alla A. Kobozeva

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

In this paper, a new approach to solving a problem of steganography algorithm stability to cover-attack is proposed. The algorithm is based on the general approach to analysis of state and functioning of information system which was previously developed by the author. Consequently, we obtain the sufficient conditions for low-sensitivity of stegano message to compression while ensuring the reliability of perception. The proposed approach automates the process of analyzing the existing or emerging steganography algorithms from viewpoint of its resistance to compression. This became possible due to estimation of singular values perturbation of cover's matrix during the stegano transformation process. Additionally the proposed algorithm allows a priori selection of less sensitive to compression stegano messages from their variety.
Keywords: steganography algorithm, compression attacks, singular values

Mathematics Subject Classification (2010) 93C40

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 1, pp. 28-35

A METHOD FOR SOLVING VARIATIONAL INEQUALITIES OF CLASS THAT USES THE OPTIMIZATION SETTING OF THE ORIGINAL PROBLEM

Sergey A. Polozhaenko[1], Alexander N. Porpulit[1], Dmitriy E. Kontreras[1], Svetlana D. Kuznichenko[2]

[1] Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: polozhaenko@mail.ru
[2] Odessa State Environmental University,
15 Lvovskaja str., Odessa, 65016, Ukraine; e-mail: kuznichenko_mail@ukr.net

The approach to the solution of the class of spatially-distributed non-steady disparities which one is offered make mathematical models of physical processes of a directional effect. The approach is grounded on optimization looked up of a maximum of a Hamiltonian function from a function of space of a condition.

Keywords: mathematical model, variation, variation inequality, optimization, principle of maximum, functional, trial function

Introduction

Analysis of physical phenomena characteristic for the class of physical processes with a pronounced directional operation (for example, the propagation of waves of different nature in heterogeneous environments, the deformation of elements of mechanical systems with variable structure, filtering highly paraffinic crude in the layers with partial conductivity of boundaries, etc.) makes it possible to consider the apparatus of variational inequalities [1-4] as an adequate mathematical description of these processes. Efficiency of approach using variation inequalities for research of processes with the directed action is grounded in more late works, for example, [7, 8].

In this paper [5] we obtain and justify a generalized mathematical model (MM) to study a class of processes, which in terms of the theory of variational inequalities can be represented as follows.

Mathematical model of process and its transformation

Let the function $\psi(t,\bar{z})$, defined on a bounded open set Ω of the space $\Re^n$, $n=1,2$, with smooth boundary Γ and the time interval $(0,t_k)$ for $t_k<\infty$, $Q=\Omega\times(0,t_k)$, $\Sigma=\Gamma\times(0,t_k)$ is the

$$\psi\in K:\left(m(\bar{z})\frac{\partial\psi}{\partial t},v-\psi\right)+\left(B(\gamma)\psi,v-\psi\right)+\mathbf{j}(v)-\mathbf{j}(u)\geq(f,v-\psi),\ \forall v\in H^1(\Omega), \qquad (1)$$

$$\psi(0,\bar{z})=\psi_0(\bar{z}), \qquad (2)$$

where the operator $B(\gamma)$ specifies a linear transformation $B(\gamma): H^1(\Omega) \to H^1(\Omega)$ and is defined by the bilinear form:

$$\left(B(\gamma)\psi, v-\psi\right) = \int_{\Omega}\left(\sum_{i=1}^{n}\frac{\partial\psi}{\partial z_i}\cdot\frac{\partial(v-\psi)}{\partial z_i}\right)d\bar{z}\,; \tag{3}$$

f — the driving function of the process, for which the operation $(f, v-\psi)$ coincides with the scalar product in $L^2(\Omega)$, i.e.

$$\left(f, v-\psi\right) = \int_{\Omega}\left[f(\bar{z}), v-\psi\right]d\Omega$$

or

$$\left(f, v-\psi\right) = \int_{\Gamma}\left[f(\bar{z}), v-\psi\right]d\Gamma$$

(hereinafter, for simplicity, restrict ourselves to the tasks at the border Γ);
$\mathbf{j}(\bullet)$ — convex functionals defining the kind of physical process in rheology and which are specified as follows

$$\begin{aligned}\mathbf{j}(\bullet) &= \int_{\Gamma}\varphi(\psi,\bar{z})\cdot\lambda(\psi)d\Gamma\,,\\ \mathbf{j}(\bullet) &= \int_{\Omega}\varphi(\psi,\bar{z})\cdot\lambda(\psi)d\Omega\,.\end{aligned} \tag{4}$$

In the relation (4) accept that $\varphi(\bullet)$ — is a continuous function, $\lambda(\bullet)$ — is continuous differentiable or not having the properties of differentiable functions.

Space of admissible functions $\varphi(\bullet)$ and $\lambda(\bullet)$ are defined as $\Delta \in L^{\infty}(\overline{Q}), \Lambda \in L^{\infty}(\overline{Q})$ where it is assumed that $\varphi(\bullet), \lambda(\bullet) \in L^{\infty}(\overline{Q})$, $\overline{Q} = \overline{\Omega}\times(0, t_k)$ and the spaces Δ and Λ are Banach with respect to the norm

$$\left\|\varphi(\psi,\bar{z})\right\|_{\Delta} = \left\|\varphi(\psi,\bar{z})\right\|_{L^{\infty}(\overline{Q})}.$$

The proposed method for solving variational inequalities of the form (1), (2) is based on the proof of the following statements.

To find the optimal solution $\psi(t,\bar{z})$ of the variational inequality (1), (2) there must exist a nonzero continuous function $p(t,\bar{z})$, so that at any time t in the interval $0 \le t \le T$ (T — time of physical processes) the Hamiltonian function $\widetilde{H}$ in the spatial domain Ω (or on its boundary Γ) would take the maximum value, where

$$\widetilde{H} = \left\langle\left(\left(B(\gamma)\widetilde{\psi}, \widetilde{v}-\widetilde{\psi}\right)+\phi(\widetilde{v})-\phi(\widetilde{\psi})-\left(\theta(\widetilde{\psi},\widetilde{v}), \widetilde{v}-\widetilde{\psi}\right)-\left(f, (\widetilde{v}-\widetilde{\psi})\right)\right), \widetilde{p}\right\rangle.$$

Carry out a preliminary series of reforms to simplify the original formulation of the problem. Introduce the notation

$$\varphi(t,\bar{z})\cdot\lambda(\psi) = \Phi(\psi), \quad \varphi(t,\bar{z})\cdot\lambda(v) = \Phi(v)$$

and

$$\phi(\psi)=\int_{\Gamma}\Phi(\psi)d\Gamma\,,\quad \phi(v)=\int_{\Gamma}\Phi(v)d\Gamma\,.$$

In addition, introduce an additional unknown function $\theta(\psi,v)$, the structure corresponding to the functionals $\mathbf{j}(\bullet)$, such that

$$(\theta(\psi,v),v-\psi)\geq 0,\ \forall v\in K\,.$$

Taking into account the executed transformations introduce the relations (1), (2) in the form

$$\psi\in K:\left(m(\bar{z})\frac{\partial\psi}{\partial t},v-\psi\right)+(B(\gamma),v-\psi)+\phi(v)-\phi(\psi)-(\theta(\psi,v),v-\psi)= \tag{5}$$
$$=(f,v-\psi),\ \forall v\in K\,,$$

$$\psi(0,\bar{z})=\psi_0(\bar{z})\,. \tag{6}$$

To solve the problem of finding a state function $\psi(t,\bar{z})$, use an optimization procedure of the Pontryagin maximum principle [6], for which choose the following performance criterion

$$J=\min\int_{\Gamma}\int_{0}^{T}|v-\psi|dtd\Gamma\,. \tag{7}$$

The physical meaning of this criterion follows from the next. The trial function $v(t,\bar{z})$ is some approximation of the unknown function $\psi(t,\bar{z})$, reflecting only the essence of physics in the specific process. Therefore, the adequacy of physical processes caused by the action of functions $v(t,\bar{z})$ and $\psi(t,\bar{z})$, is provided up to the accuracy within the difference between these functions. In this case, the integral difference between the trial $v(t,\bar{z})$ and the unknown $\psi(t,\bar{z})$ functions can be regarded as a quantitative measure or a penalty for the deviation of the actual flow of the process from its true value.

Obtain the necessary optimality conditions of the problems (5) (6), (7).

According to [6], introduce a new coordinate

$$\frac{\partial^2\sigma}{\partial t\partial z}=|v-\psi|^2\Big|_{z\in\Gamma}\,. \tag{8}$$

Thus, the original problem will be considered in $(n+1)$-dimensional space with the equation of dynamics

$$\widetilde{\psi}\in K:\left(m(\bar{z})\frac{\partial\widetilde{\psi}}{\partial t},\widetilde{v}-\widetilde{\psi}\right)+(B(\gamma),\widetilde{v}-\widetilde{\psi})+\phi(\widetilde{v})-\phi(\widetilde{\psi})-(\theta(\widetilde{\psi},\widetilde{v}),\widetilde{v}-\widetilde{\psi})= \tag{9}$$
$$=(f,\widetilde{v}-\widetilde{\psi}),\ \forall\widetilde{v}\in K$$

where

$$\tilde{\psi} = (\sigma, \psi_1, ..., \psi_n), \quad \tilde{v} = (\sigma, v_1, ..., v_n)$$

with the initial conditions

$$\tilde{\psi}(0, \bar{z}) = [0, \psi_0(\bar{z})].$$

Assume that we have found $\psi(t, \bar{z})$. This condition corresponds to the relation

$$\min \int_{\Gamma} \int_{0}^{T} |\tilde{v} - \tilde{\psi}|^2 \, dt \, d\Gamma \to J_{\min} = J^*.$$

At $t = \tau \ (0 \le \tau \le T)$ perform a needle-shaped variation with the duration ε. As a result of the variation performed the value of the functional J (7) changes

$$\hat{J} = \int_{\Gamma} \int_{0}^{T} |\tilde{v} - \tilde{\psi}| \, dt \, d\Gamma > J_{\min}.$$

Write down the detailed result of the variation

$$\begin{aligned} \delta\tilde{v} = \tilde{v} - \tilde{\psi} = \varepsilon \{ [(B(\gamma)\tilde{\psi}, \tilde{v} - \tilde{\psi}) + \phi(\tilde{v}) - \phi(\tilde{\psi}) - (\theta(\tilde{\psi}, \tilde{v}), \tilde{v} - \tilde{\psi}) - (f, (\tilde{v} - \tilde{\psi}))] - \\ - (B(\gamma)\tilde{\psi}, \psi) + \phi(\tilde{\psi}) - (\theta(\tilde{\psi}), \tilde{\psi}) - (f, \tilde{\psi}) \}_{t=\tau}. \end{aligned} \tag{10}$$

Express $\tilde{v}$ through the variation and optimal function of the state

$$\tilde{v} = \tilde{\psi} + \delta\tilde{v}. \tag{11}$$

Substituting (11) into (9), obtain

$$\begin{aligned} \tilde{\psi} \in K : \left(m(\bar{z}) \frac{\partial \tilde{\psi}}{\partial t}, (\tilde{\psi} + \delta\tilde{v}) - \tilde{\psi} \right) = (B(\gamma)\tilde{\psi}, (\tilde{\psi} + \delta\tilde{v}) - \tilde{\psi}) + \phi(\tilde{\psi} + \delta\tilde{v}) - \phi(\tilde{\psi}) - \\ - (\theta(\tilde{\psi}, (\tilde{\psi} + \delta\tilde{v})), (\tilde{\psi} + \delta\tilde{v}) - \tilde{\psi}) - (f, (\tilde{\psi} + \delta\tilde{v}) - \tilde{\psi}), \ \forall \tilde{v} \in K. \end{aligned} \tag{12}$$

For further transformations use the coordinate-wise analog (12)

$$\begin{aligned} \tilde{\psi}_i \in K : \left(m(\bar{z}_i) \frac{\partial \tilde{\psi}_i}{\partial t}, (\tilde{\psi}_i + \delta\tilde{v}_i) - \tilde{\psi}_i \right) = (B(\gamma)\tilde{\psi}_i, (\tilde{\psi}_i + \delta\tilde{v}_i) - \tilde{\psi}_i) + \phi(\tilde{\psi}_i + \delta\tilde{v}_i) - \\ - \phi(\tilde{\psi}_i) - (\theta(\tilde{\psi}_i, (\tilde{\psi}_i + \delta\tilde{v}_i)), (\tilde{\psi}_i + \delta\tilde{v}_i) - \tilde{\psi}_i) - (f, (\tilde{\psi}_i + \delta\tilde{v}_i) - \tilde{\psi}_i), \\ \forall \tilde{v}_i \in K, \quad i = 0, 1, ..., n. \end{aligned} \tag{13}$$

Expand (13) in Taylor series and restrict the consideration with the quantities of first-order of infinitesimality

$$m(z_i)\left(\frac{\partial\tilde{\psi}_i}{\partial t}+\frac{\partial\tilde{v}_i}{\partial t}\right)=\left(B(\gamma)\tilde{\psi}_i,\tilde{\psi}_i\right)+\phi(\tilde{\psi}_i)-(f,\tilde{\psi}_i)+$$

$$\sum_{i=0}^{n}\frac{\partial\left[\left(B(\gamma)\tilde{\psi}_i,\tilde{\psi}_i\right)_i+\phi(\tilde{\psi}_i)-(f,\tilde{\psi}_i)\right]}{\partial\tilde{v}_i}\delta\tilde{v}_i, \tag{14}$$

$$i=0,1,...,n.$$

From (14) it follows that

$$m(z_i)\frac{\partial\tilde{v}_i}{\partial t}=\sum_{i=0}^{n}\frac{\partial\left[\left(B(\gamma)\tilde{\psi}_i,\tilde{\psi}_i\right)+\phi(\tilde{\psi}_i)-(f,\tilde{\psi}_i)\right]}{\partial\tilde{v}_i}\delta\tilde{v}_i,\quad i=0,1,...,n. \tag{15}$$

Now turn to $t=T$. Define a variation of the functional at $t=T$

$$\delta J_{t=T}=\hat{J}-J_{\min}>0$$

or

$$-\delta J_{t=T}=-\delta\sigma_{t=T}\le 0.$$

Introduce the variable $\tilde{p}(t,\bar{z})$ so that when $t=T$ this condition is satisfied

$$-\delta J_{t=T}=-\delta\sigma(T)=\left\langle\delta\tilde{v},\tilde{p}\right\rangle_{t=T}. \tag{16}$$

Coordinate-wise analog (16) is as follows

$$-\delta J_{t=T}=-\delta\sigma(T)=\left\langle\delta\tilde{v}_i,\tilde{p}_i\right\rangle_{t=T},\quad i=0,1,...,n.$$

Since $\delta\sigma(T)>0$, in order to satisfy this relation there should take place:

$$p^0(T,\bar{z}_i)=-1;\qquad p_j(T,\bar{z})=0,$$

where $i=0,1,...,n;\ j=1,...,n$.

Thus, if the optimal solution is not found, then $-\delta J<0$, and for the optimal solution $-\delta J=0$ is valid, since the variation of functional must be zero for the optimal solution.

Associate a variable $\tilde{p}(t,\bar{z})$ to the dynamic equation of the process observed through trial function $v(t,\bar{z})$. Find a variable $\tilde{p}(t,\bar{z})$ which satisfies

$$\left\langle\delta\tilde{v}(t,\bar{z}),\tilde{p}(t,\bar{z})\right\rangle=\left\langle\delta\tilde{v}(T,\bar{z}),\tilde{p}(T,\bar{z})\right\rangle_{t-\varepsilon\le t\le T}=const.$$

Then we have

$$\frac{\partial}{\partial t}\left\langle\delta\tilde{v}(t,\bar{z}),\tilde{p}(t,\bar{z})\right\rangle=\left\langle\frac{\partial\,\delta\tilde{v}(t,\bar{z})}{\partial t},\tilde{p}(t,\bar{z})\right\rangle+\left\langle\frac{\partial\,v\tilde{p}(t,\bar{z})}{\partial t},\delta\tilde{v}(t,\bar{z})\right\rangle_{t-\varepsilon\le t\le T}=0. \tag{17}$$

Coordinate-wise analog (17) is

$$\sum_{i=0}^{n}\frac{\partial\,\delta\widetilde{v}_i(t,\bar{z})}{\partial t}\widetilde{p}_i(t,\bar{z})+\sum_{i=0}^{n}\delta\widetilde{v}_i(t,\bar{z})\frac{\partial\,\widetilde{p}_i\widetilde{v}_i(t,\bar{z})}{\partial t}=0,\quad i=0,1,...,n. \tag{18}$$

Substitute in (18) the value of the derivative $\dfrac{\partial\,\delta\widetilde{v}(t,\bar{z})}{\partial t}$ from (15)

$$m(z_i)\sum_{i=0}^{n}\widetilde{p}_i\times\sum_{i=0}^{n}\frac{\partial\left[\left(B(\gamma)\widetilde{\psi}_i,\widetilde{\psi}_i\right)+\phi(\widetilde{\psi}_i)-\left(f,\widetilde{\psi}_i\right)\right]}{\partial\,\widetilde{v}_i}\delta\widetilde{v}_i+\sum_{i=0}^{n}\delta\widetilde{v}_i\frac{\partial\,\widetilde{p}}{\partial t}=0,\quad i=0,1,...,n \tag{19}$$

Change the order of summation in (19)

$$m(z_i)\sum_{i=0}^{n}\delta\widetilde{v}_i+\left[\sum_{i=0}^{n}\widetilde{p}_i\frac{\partial\left[\left(B(\gamma)\widetilde{\psi}_i,\widetilde{\psi}_i\right)+\phi(\widetilde{\psi}_i)-\left(f,\widetilde{\psi}_i\right)\right]}{\partial\,\widetilde{v}_i}+\frac{\partial\,\widetilde{p}_i}{\partial t}\right]=0,\quad i=0,1,...,n.$$

Finally get

$$\frac{\partial\,\widetilde{p}_i}{\partial t}=-\sum_{i=0}^{n}\frac{\partial\left[\left(B(\gamma)\widetilde{\psi}_i,\widetilde{\psi}_i\right)+\phi(\widetilde{\psi}_i)-\left(f,\widetilde{\psi}_i\right)\right]}{\partial\,\widetilde{v}_i}\widetilde{p}_i,\quad i=0,1,...,n.$$

Note that this equation is the dual of (5), and the variable $\widetilde{p}(t,\bar{z})$ is expressed through the function of phase.

Again turn to the variation of functional (7) at $t=T$

$$-\delta J_{t=T}=\left\langle\delta\widetilde{v}(t,\bar{z}),\widetilde{p}(t,\bar{z})\right\rangle_{t=T}=0.$$

Replace the variation $\delta\widetilde{v}$ with the value of (10), reduce by ε and, since τ can be arbitrary, obtain

$$\begin{gathered}\left\langle\left(\left(B(\gamma)\widetilde{\psi},\widetilde{v}-\widetilde{\psi}\right)+\phi(\widetilde{v})-\phi(\widetilde{\psi})-\left(\theta(\widetilde{\psi},\widetilde{v}),\widetilde{v}-\widetilde{\psi}\right)-\left(f,(\widetilde{v}-\widetilde{\psi})\right)\right),\widetilde{p}\right\rangle_{t=\tau}-\\-\left\langle\left(\left(B(\gamma)\widetilde{\psi},\widetilde{\psi}\right)+\phi(\widetilde{\psi})-\left(f,\widetilde{\psi}\right)\right),\widetilde{p}\right\rangle_{t=T}=0.\end{gathered} \tag{20}$$

From (20) it follows that the second summand in it corresponds to the optimal solution of the variational inequality (5). In the case when the optimal solution $\psi(t,\bar{z})$ is found, variation of functional J will be zero, i.e. $\delta J=0$. Given this, the first summand in (20), defined by the Hamiltonian function

$$\widetilde{H}=\left\langle\left(\left(B(\gamma)\widetilde{\psi},\widetilde{v}-\widetilde{\psi}\right)+\phi(\widetilde{v})-\phi(\widetilde{\psi})-\left(\theta(\widetilde{\psi},\widetilde{v}),\widetilde{v}-\widetilde{\psi}\right)-\left(f,(\widetilde{v}-\widetilde{\psi})\right)\right),\widetilde{p}\right\rangle \tag{21}$$

should take the maximum value. Thus, the above statement is proven. Let's show the possibility of determining the maximum value of Hamiltonian function.

Coordinate-wise analog (21) is defined by

$$\begin{gathered}\widetilde{H}=\left\langle\left(\left(B(\gamma)\widetilde{\psi}_i,\widetilde{v}_i-\widetilde{\psi}_i\right)+\phi(\widetilde{v}_i)-\phi(\widetilde{\psi}_i)-\left(\theta(\widetilde{\psi}_i,\widetilde{v}_i),\widetilde{v}_i-\widetilde{\psi}_i\right)-\left(f,(\widetilde{v}_i-\widetilde{\psi}_i)\right)\right),\widetilde{p}_i\right\rangle,\\i=0,1,...,n.\end{gathered} \tag{22}$$

To maximize the value of the function $\widetilde{H}$, it's necessary to set all the partial derivatives of this function to zero by a testing variable $v(t,\bar{z})$, that taking into account (22) gives the system of equations

$$\frac{\partial \widetilde{H}}{\partial v_i} = 0, \quad i = 0,1,...,n. \tag{23}$$

Coordinate wise analog (22) contains $(n+1)$ of v_i functions, $(n+1)$ of θ_i functions and $(n+1)$ of p_i functions. Since the equations (23) are only $(n+1)$, and the unknown are $(3n+3)$, then the system (23) cannot be solved. To solve (23) define also the partial derivatives

$$\frac{\partial \widetilde{H}}{\partial \theta_i} = \widetilde{p}_i, \quad i = 0,1,...,n; \tag{24}$$

$$\frac{\partial \widetilde{H}}{\partial p_i} = \left[m(\bar{z}_i)\frac{\partial \widetilde{\psi}_i}{\partial t}, \widetilde{v}_i - \widetilde{\psi}_i \right], \quad i = 0,1,...,n. \tag{25}$$

In this case, the solution of (23) can be obtained.

As a result of the reasoning done, the scheme of the algorithm for solving variational inequality (5) using the maximum principle can be represented as follows:

1) The dynamic equation (9), subject to the additional coordinate σ is written down.

2) An auxiliary function (Hamilton) $\widetilde{H}$ in accordance with the expression (22) is compiled.

3) A test function $v(t,\bar{z})$ that delivers maximum $\widetilde{H}$ functions in accordance with the expression (23) is determined. For the redefinition of the independent variables θ and p the system (23) is supplemented with equations (24) and (25).

4) The unknown variable $\psi(t,\bar{z})$ is determined by the test variable $v(t,\bar{z})$, which gives the maximum value of functions $\widetilde{H}$.

Conclusion

Thus, a method and an algorithm implementing it is proposed for solving a class of variational inequalities, which are mathematical models of the above physical processes with a pronounced directional effect. The proposed method is based on the optimization procedure of the maximum principle. The choice of optimality criterion for solving the external problem is justified.

References

1. Duvaut G. Inequalities in Mechanics and Physics / G. Duvant, J.-L. Lions. – Berlin ; New York : Springer-Verlag, 1976. – 397 p. – (Russian Translation Nauka Moscow, 1980).
2. Kinderlehrer D. An Introduction to Variational Inequalities and Their Applications / D. Kinderlehrer, G. Stampacchia. – New York : Academic Press, 1980. – 313 p. – (Russian Translation MIR Publ. Moscow, 1983).
3. Panagiotopoulos P.D. Inequalities Problems in Mechanics and Applications. Convex and Nonconvex Energy Function. – Boston : Birkhäuser, 1985. – 412 p. – (Russian Translation MIR Publ. Moscow, 1989).

4. Bernadiner M.G. Hydrodynamic Theory of Filtration of Anomalous Liquids / M.G. Bernadiner, V.M. Entov. – M. : Nauka, 1975. – 199 p. – (in Russian).
5. Polozhaenko S.A. Mathematical models of the flow of anomalous fluids // Simulation and information technology. – 2001. – Vol.9. – PP. 14-21. – (in Russian).
6. Pontryagin L.S. et al. The Mathematical Theory of Optimal Processes. – Moscow : Gosudarstv. Izdat. Fiz.-Mat. Lit., 1961. – 391 p. – (in Russian).
7. Sofonea M. Variational Inequalities With Applications: A Study of Antiplane Frictional Contact Problems / M. Sofonea, A. Matei. – New York : Springer Verlag, 2009. – 230 p.
8. Dostál Z. Optimal Quadratic Programming Algorithms. With Applications to Variational Inequalities. – New York : Springer, 2009. – 284 p.

МЕТОД РОЗВ'ЯЗАННЯ ОДНОГО КЛАСУ ВАРІАЦІЙНИХ НЕРІВНОСТЕЙ, ЗАСНОВАНИЙ НА ВИКОРИСТАННІ ОПТИМІЗАЦІЙНОЇ ПРОЦЕДУРИ

С.А. Положаєнко[1], О.М. Порпуліт[1], Д.Е. Контрерас[1], С.Д. Кузніченко[2]

[1] Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: polozhaenko@mail.ru
[2] Одеський державний екологічний університет,
вул. Львівська, 15, Одеса, 65016, Україна; e-mail: kuznichenko_mail@ukr.net

Розглянуто розв'язки класу задач просторово-розподілених нестаціонарних фізичних процесів з однобічною провідністю. Пошук розв'язків ґрунтуються на застосуванні оптимізаційної процедури методу максимуму функції Гамільтона від змінних просторових координат.
Ключові слова: математична модель, варіація, варіаційна нерівність, оптимізація, принцип максимуму, функціонал, шукана функція

МЕТОД РЕШЕНИЯ ОДНОГО КЛАССА ВАРИАЦИОННЫХ НЕРАВЕНСТВ, ОСНОВАННЫЙ НА ИСПОЛЬЗОВАНИИ ПРОЦЕДУРЫ ОПТИМИЗАЦИИ

С.А. Положаенко[1], А.Н. Порпулит[1], Д.Э. Контрерас[1], С.Д. Кузниченко[2]

[1] Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: polozhaenko@mail.ru
[2] Одесский государственный экологический университет,
ул. Львовская, 15, Одесса, 65016, Украина; e-mail: kuznichenko_mail@ukr.net

Рассмотрено решение класса задач пространственно-распределенных нестационарных физических процессов с односторонней проводимостью. Поиск решения основан на применении оптимизационной процедуры метода максимума функции Гамильтона от переменных пространственных координат.
Ключевые слова: математическая модель, вариация, вариационное неравенство, оптимизация, принцип максимума, функционал, искомая функция

УДК 351.746.1:001

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 1, pp. 36-45

ОБҐРУНТУВАННЯ АЛГОРИТМУ ВІДШУКАННЯ ЗНАЧЕНЬ ІНТЕНСИВНОСТЕЙ ВІДМОВ І ВІДНОВЛЕНЬ ТЕХНІЧНИХ СИСТЕМ НА ОСНОВІ ЗАСТОСУВАННЯ МЕТОДІВ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ

О.В. Боровик[1], Г.Б. Жиров[2], І.В. Гащук[1]

[1] Національна академія Державної прикордонної служби України імені Б. Хмельницького, вул. Шевченка, 46, Хмельницький, 29003, Україна

[2] Військовий інститут Київського національного університету імені Тараса Шевченка, просп. Глушкова, 2, корпус 8, Київ, 03680, Україна

У роботі запропоновано новий підхід до визначення інтенсивностей відмов і відновлень складних технічних систем довільної природи, що базується на застосуванні методів теорії ймовірностей, математичної статистики, імітаційного моделювання та апроксимації функцій. Відшукання інтенсивностей відмов і відновлень у вигляді функціональних залежностей дозволяє здійснити моделювання функції готовності.

Ключові слова: інтенсивність відмов, інтенсивність відновлень, технічна система, імітаційне моделювання, алгоритм

Вступ

У моделюванні випадкових процесів з дискретними станами та неперервним часом, що характерні для технічних систем (ТС) у процесі їх експлуатації, одними з найважливіших показників, що визначають функцію готовності ТС, є їх інтенсивності відмов і відновлень. Стаціонарні, або однорідні за часом, марковські процеси відмов-відновлень елементів ТС характеризуються постійними умовними щільностями (інтенсивностями) розподілів відмов і відновлень λ, μ. Теорія таких процесів та її застосування у питаннях надійності розглянуті у багатьох працях, зокрема в [1-3]. Значно менше уваги дослідники приділили нестаціонарним марковським процесам, що обумовлені змінними у часі інтенсивностями $\lambda(t)$, $\mu(t)$. Однак саме вони більш адекватні реальним умовам експлуатації ТС. Саме тому в попередніх роботах авторів вже розглядалися питання теорії надійності ТС на основі аналізу згаданих процесів як нестаціонарних марковських [4]. У цих працях висувалося припущення про лінійний вид залежностей для $\lambda(t)$, $\mu(t)$, що відповідало розглядуваним типам ТС, проте не мало властивості універсальності. Це призводило до конкретизації розрахункової процедури відшукання значень функції готовності, що мало підходить для інших типів ТС та краще застосовується для ручного розрахунку. Однак важливим завданням є отримання універсальної теорії і методики її застосування до технічних систем довільної природи за відсутності обмежень і мінімізації припущень щодо виду залежностей для $\lambda(t)$, $\mu(t)$.

Мета статті і постановка досліджень

Враховуючи важливість знання інтенсивностей відмов і відновлень складних технічних систем для відшукання функції готовності та обґрунтування заходів адаптивної системи експлуатації, важливим завданням є опрацювання підходу до їх визначення для технічних систем довільної природи на основі знання статистичних даних щодо відмов-відновлень складових систем і відсутності припущень щодо виду залежностей для $\lambda(t)$, $\mu(t)$.

Виклад основного матеріалу дослідження

Для досягнення визначеної мети розглянемо m однотипних технічних пристроїв або складних технічних систем (цю сукупність у подальшому позначатимемо, як ТС), що експлуатуються в однакових умовах. Їх працездатний стан характеризується працездатним станом складових елементів і перебуванням відповідних характеристичних параметрів у допустимих межах. Розглянемо роботу ТС протягом певного проміжку часу $[0;T_k]$, де T_k – кінцевий момент експлуатації зразка ТС за технічною документацією.

Здійснимо розбиття проміжку часу $[0;T_k]$ на n рівних часткових інтервалів довжиною Δt точками $t_i, \left(i=\overline{0;n}\right)$.

Для кожного моменту часу $t_i, \left(i=\overline{0;n}\right)$ j-го ($j=\overline{1;m}$) зразка ТС можна отримати статистичну інформацію про стан його складових елементів і характеристичних параметрів. Ця інформація може бути систематизована у вигляді, що наведений у табл. 1-4.

Таблиця 1.

j / $(t_i;t_i+\Delta t]$	1	2	…	m
$(t_0;t_0+\Delta t]$	$n_1(t_0,t_0+\Delta t)$	$n_2(t_0,t_0+\Delta t)$	…	$n_m(t_0,t_0+\Delta t)$
$(t_1;t_1+\Delta t]$	$n_1(t_1,t_1+\Delta t)$	$n_2(t_1,t_1+\Delta t)$	…	$n_m(t_1,t_1+\Delta t)$
…	…	…	…	…
$(t_{n-1};t_{n-1}+\Delta t]$	$n_1(t_{n-1},t_{n-1}+\Delta t)$	$n_2(t_{n-1},t_{n-1}+\Delta t)$	…	$n_m(t_{n-1},t_{n-1}+\Delta t)$

У табл. 1 $n_j(t_i,t_i+\Delta t)$ – кількість елементів (параметрів) j-го зразка ТС, що відмовили за проміжок часу $(t_i;t_i+\Delta t]$.

Таблиця 2.

j / t_i	1	2	…	m
t_0	$N_1(t_0)$	$N_2(t_0)$	…	$N_m(t_0)$
t_1	$N_1(t_1)$	$N_2(t_1)$	…	$N_m(t_1)$
…	…	…	…	…
t_{n-1}	$N_1(t_{n-1})$	$N_2(t_{n-1})$	…	$N_m(t_{n-1})$

У табл. 2 $N_j(t_i)$ – кількість справних елементів (параметрів) *j*-го зразка ТС на момент часу t_i.

Таблиця 3.

j / $(t_i;t_i+\Delta t]$	1	2	…	m
$(t_0;t_0+\Delta t]$	$\Delta m_1(t_0,t_0+\Delta t)$	$\Delta m_2(t_0,t_0+\Delta t)$	…	$\Delta m_m(t_0,t_0+\Delta t)$
$(t_1;t_1+\Delta t]$	$\Delta m_1(t_1,t_1+\Delta t)$	$\Delta m_2(t_1,t_1+\Delta t)$	…	$\Delta m_m(t_1,t_1+\Delta t)$
…	…	…	…	…
$(t_{n-1};t_{n-1}+\Delta t]$	$\Delta m_1(t_{n-1},t_{n-1}+\Delta t)$	$\Delta m_2(t_{n-1},t_{n-1}+\Delta t)$	…	$\Delta m_m(t_{n-1},t_{n-1}+\Delta t)$

У табл. 3 $\Delta m_j(t_i,t_i+\Delta t)$ – кількість елементів (параметрів) *j*-го зразка ТС, що відновлені за проміжок часу $(t_i;t_i+\Delta t]$.

Таблиця 4.

j / t_i	1	2	…	m
t_0	$M_1(t_0)$	$M_2(t_0)$	…	$M_m(t_0)$
t_1	$M_1(t_1)$	$M_2(t_1)$	…	$M_m(t_1)$
…	…	…	…	…
t_{n-1}	$M_1(t_{n-1})$	$M_2(t_{n-1})$	…	$M_m(t_{n-1})$

У табл. 4 $M_j(t_i)$ – кількість невідновлених елементів (параметрів) *j*-го зразка ТС на момент часу t_i.

На основі даних табл. 1-4 нескладно знайти інтенсивності відмов і відновлень для кожного зразка досліджуваної сукупності ТС і кожного з досліджуваних моментів часу. Для цього слід скористатися наступними залежностями [3]:

$$\lambda_j^*(t_i)=\frac{n_j(t_i,t_i+\Delta t)}{N_j(t_i)\cdot\Delta t}, \qquad (1)$$

$$\mu_j^*(t_i)=\frac{\Delta m_j(t_i,t_i+\Delta t)}{M_j(t_i)\cdot\Delta t}. \qquad (2)$$

Сукупність знайдених на основі даних табл. 1-4 і залежностей (1), (2) інтенсивностей відмов і відновлень може бути оцінена з табл. 5, 6.

Знання даних табл. 5, 6 дозволяє встановити закон розподілу інтенсивності відмов і відновлень досліджуваної сукупності ТС для кожного досліджуваного моменту часу. Для інтенсивності відмов здійснюється це наступним чином. Для кожного $i=const$, тобто для фіксованого значення t_i, та для $j=\overline{1;m}$ формується статистичний ряд з величин $\lambda_j^*(t_i)$. На його основі будується гістограма частот величин $\lambda_j^*(t_i)$. Її форма дозволяє висунути гіпотезу про закон розподілу величини $\lambda^*(t_i)$, яка являє собою інтенсивність відмов досліджуваної сукупності ТС для фіксованого моменту часу t_i.

Застосування непараметричних і параметричних критеріїв [5] дозволяє перевірити цю гіпотезу та знайти параметри законів розподілу й представити ці закони у вигляді $F_i\left(\lambda^*(t_i)\right)$.

Таблиця 5.

t_i \ j	1	2	…	m
t_0	$\lambda_1^*(t_0)$	$\lambda_2^*(t_0)$	…	$\lambda_m^*(t_0)$
t_1	$\lambda_1^*(t_1)$	$\lambda_2^*(t_1)$	…	$\lambda_m^*(t_1)$
…	…	…	…	…
t_{n-1}	$\lambda_1^*(t_{n-1})$	$\lambda_2^*(t_{n-1})$	…	$\lambda_m^*(t_{n-1})$

Таблиця 6.

t_i \ j	1	2	…	m
t_0	$\mu_1^*(t_0)$	$\mu_2^*(t_0)$	…	$\mu_m^*(t_0)$
t_1	$\mu_1^*(t_1)$	$\mu_2^*(t_1)$	…	$\mu_m^*(t_1)$
…	…	…	…	…
t_{n-1}	$\mu_1^*(t_{n-1})$	$\mu_2^*(t_{n-1})$	…	$\mu_m^*(t_{n-1})$

Застосовуючи аналогічний підхід, можна знайти закони розподілу інтенсивності відновлень досліджуваної сукупності ТС для кожного досліджуваного моменту часу та представити їх у вигляді $F_i\left(\mu^*(t_i)\right)$. Процедура відшукання законів розподілу інтенсивності відмов і відновлень досліджуваної сукупності ТС для кожного досліджуваного моменту часу може бути оцінена з рис. 1, 2, відповідно.

Знання законів розподілу інтенсивності відмов $F_i\left(\lambda^*(t_i)\right)$ і відновлень $F_i\left(\mu^*(t_i)\right)$ досліджуваної сукупності ТС для кожного досліджуваного моменту часу t_i дозволяє встановити безпосередньо значення інтенсивностей відмов $\lambda^*(t_i)$ і відновлень $\mu^*(t_i)$ досліджуваної сукупності ТС для кожного досліджуваного моменту часу t_i. Для цього можна застосувати методи імітаційного моделювання [1]. Технічний аспект їх використання може бути наступним.

Для того, щоб провести імітацію, яка б забезпечила достатньо достовірні результати, потрібно насамперед встановити необхідну кількість реалізацій $k_н$. Для цього слід провести попередні розрахунки, суть яких така. Фіксується попередня певна кількість реалізацій q. Далі розігрується q разів випадкове число $R \in [0;1]$. На основі використання функцій $F_i\left(\lambda^*(t_i)\right)$ розігруються значення $\left(\lambda^*(t_i)\right)_l$ для l-ї реалізації $\left(l = \overline{1;q}\right)$ за наступним принципом. Приймається, що $F_i\left(\lambda^*(t_i)\right) = R$ і знаходяться значення $\left(\lambda^*(t_i)\right)_l$ за наступною формулою:

$$\left(\lambda^*(t_i)\right)_l = F_i^{-1}(R) \qquad (3)$$

де $F_i^{-1}(R)$ – функція, що обернена до функції $F_i\left(\lambda^*(t_i)\right)$.

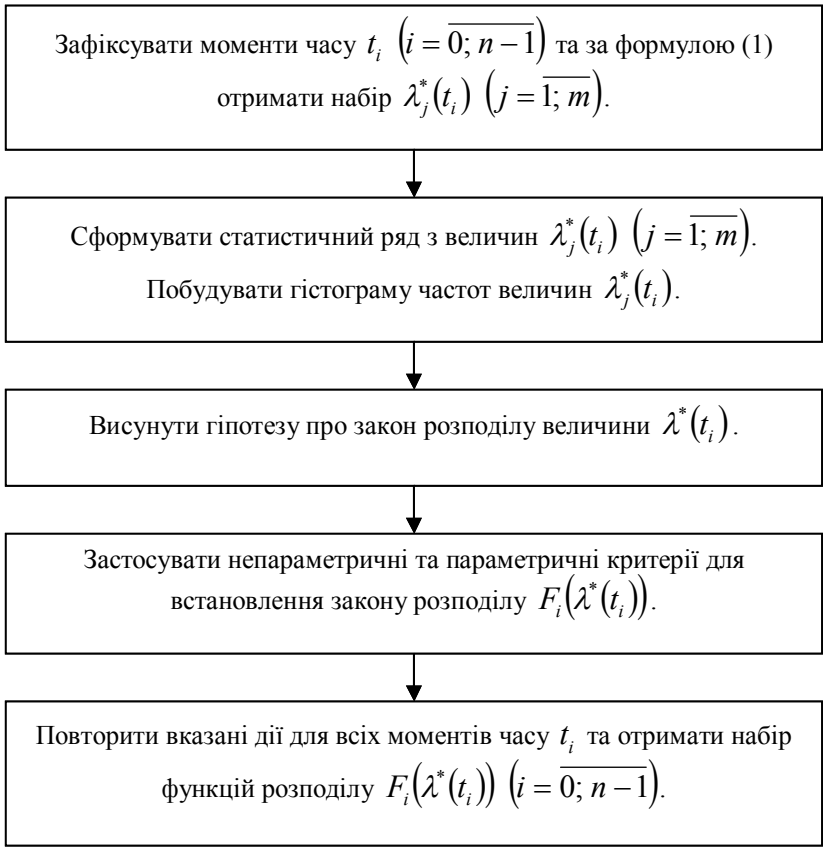

Рис. 1. Схема відшукання законів розподілу інтенсивності відмов сукупності ТС

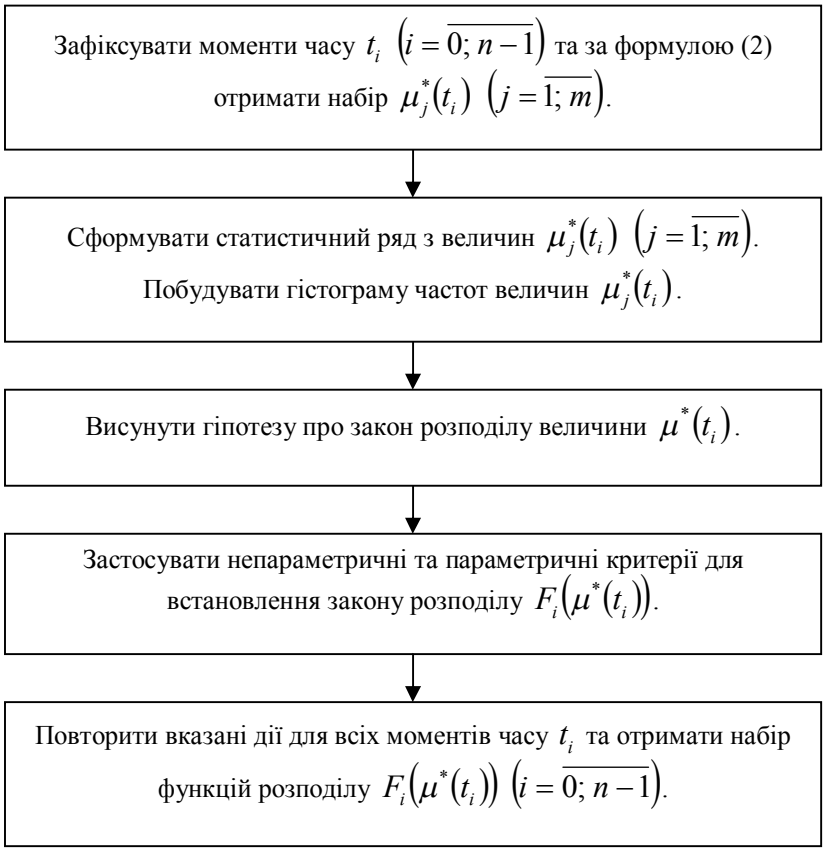

Рис. 2. Схема відшукання законів розподілу інтенсивності відновлень сукупності ТС

Принцип відшукання значень $\left(\lambda^*(t_i)\right)_l$ при *l*-й реалізації можна оцінити з рис. 3.

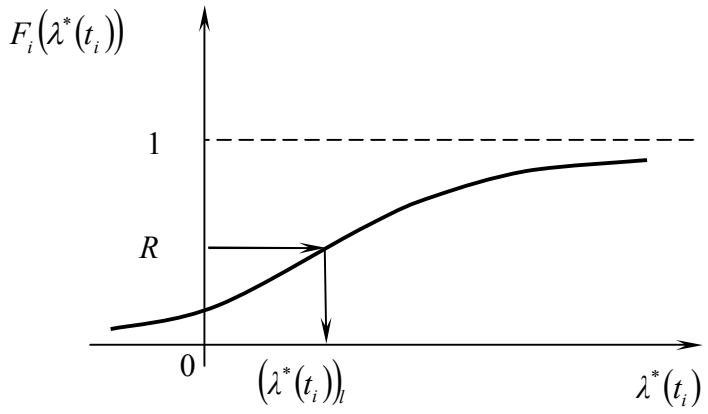

Рис. 3. Принцип відшукання значень $\left(\lambda^*(t_i)\right)_l$

Результати розіграшів значень $\left(\lambda^*(t_i)\right)_l$ для всіх реалізацій l, $\left(l=\overline{1;q}\right)$ можуть бути оцінені з табл. 7.

Таблиця 7.

Номер реалізації / t_i	1	2	…	q
t_0	$\left(\lambda^*(t_0)\right)_1$	$\left(\lambda^*(t_0)\right)_2$	…	$\left(\lambda^*(t_0)\right)_q$
t_1	$\left(\lambda^*(t_1)\right)_1$	$\left(\lambda^*(t_1)\right)_2$	…	$\left(\lambda^*(t_1)\right)_q$
…	…	…	…	…
t_{n-1}	$\left(\lambda^*(t_{n-1})\right)_1$	$\left(\lambda^*(t_{n-1})\right)_2$	…	$\left(\lambda^*(t_{n-1})\right)_q$

Використання даних табл. 7 дозволяє відшукати середні значення інтенсивностей відмов $\overline{\lambda^*(t_i)}$ досліджуваної сукупності ТС для кожного досліджуваного моменту часу t_i при q реалізаціях. Для цього слід урахувати, що для кожного моменту часу t_i всі реалізації є рівнозначними, а отже, величини $\overline{\lambda^*(t_i)}$ можуть бути знайдені за наступною формулою:

$$\overline{\lambda^*(t_i)}=\frac{1}{q}\cdot\sum_{l=1}^{q}\left(\lambda^*(t_i)\right)_l,\ \left(i=\overline{0;n-1},\ i=const\right). \qquad (4)$$

Однак ці величини ще не визначають значення інтенсивностей відмов $\lambda^*(t_i)$ досліджуваної сукупності ТС для кожного досліджуваного моменту часу t_i з достатньою достовірністю. Для забезпечення останньої необхідно здійснити розрахунки величини $\lambda^*(t_i)$ за формулою (4) однак при значенні $q=k_н$, яке б забезпечувало за певним рівнем довіри Q достовірність значень $\lambda^*(t_i)$.

Для знаходження $k_н$ пропонується скористатися формулою

$$k_н = \max\{k_н(t_0),\ldots,k_н(t_{n-1})\}. \quad (5)$$

В останній $k_н(t_i)$ – це такі кількості реалізацій (розіграшів випадкових чисел $R \in [0;1]$), які можуть забезпечити достатньо достовірні за вибраним рівнем довіри Q значення $\lambda^*(t_i)$. При цьому значення $k_н(t_i)$ можуть бути знайдені наступним чином [1]:

$$k_н(t_i) = \left(\frac{\sigma_{\overline{\lambda^*(t_i)}}}{\varepsilon}\right)^2 \left[\Phi^{-1}\left(\frac{1}{2}Q\right)\right]^2, \left(i = \overline{0;n-1},\ i = const\right). \quad (6)$$

У формулі (6) $\sigma_{\overline{\lambda^*(t_i)}}$ – це величина, що знаходиться, як [1]:

$$\sigma_{\overline{\lambda^*(t_i)}} \approx \sqrt{\frac{1}{q}\sum_{l=1}^{q}\left(\lambda^*(t_i)\right)_l^2 - \overline{\lambda^*(t_i)}^2}, \left(i = \overline{0;n-1},\ i = const\right), \quad (7)$$

де

$\Phi^{-1}\left(\frac{1}{2}Q\right)$ – функція, що обернена до функції Лапласа (її значення для деяких, найбільш типових значень рівня довіри Q можуть бути оцінені з табл. 8);

ε – рівень похибки, що характеризує відхилення середнього арифметичного величини $\lambda^*(t_i)$ від її математичного сподівання.

Якщо якась з величин $k_н(t_i)$ виявиться не цілим числом, то її необхідно округлити в більшу сторону.

Таблиця 8.

Q	0.80	0.85	0.90	0.95	0.96	0.97
$\left[\Phi^{-1}\left(\frac{1}{2}Q\right)\right]^2$	1.64	2.08	2.71	3.84	4.21	4.49
Q	0.98	0.99	0.995	0.999	0.9995	0.9999
$\left[\Phi^{-1}\left(\frac{1}{2}Q\right)\right]^2$	5.43	6.61	7.90	10.9	12.25	15.2

Коректність формули (5) випливає з того, що якщо при меншій кількості реалізацій забезпечується достовірність значень $\lambda^*(t_i)$, то при більшій кількості реалізацій це значення тим більш буде достовірним.

Знання величини $k_н$ дозволяє відшукати значення інтенсивностей відмов $\lambda^*(t_i)$ досліджуваної сукупності ТС для кожного досліджуваного моменту часу t_i за наступною формулою:

$$\lambda^*(t_i) = \frac{1}{k_н}\cdot\sum_{l=1}^{k_н}\left(\lambda^*(t_i)\right)_l, \left(i = \overline{0;n-1},\ i = const\right). \quad (8)$$

Процедура відшукання значень $\lambda^*(t_i)$ може бути оцінена з рис. 4.

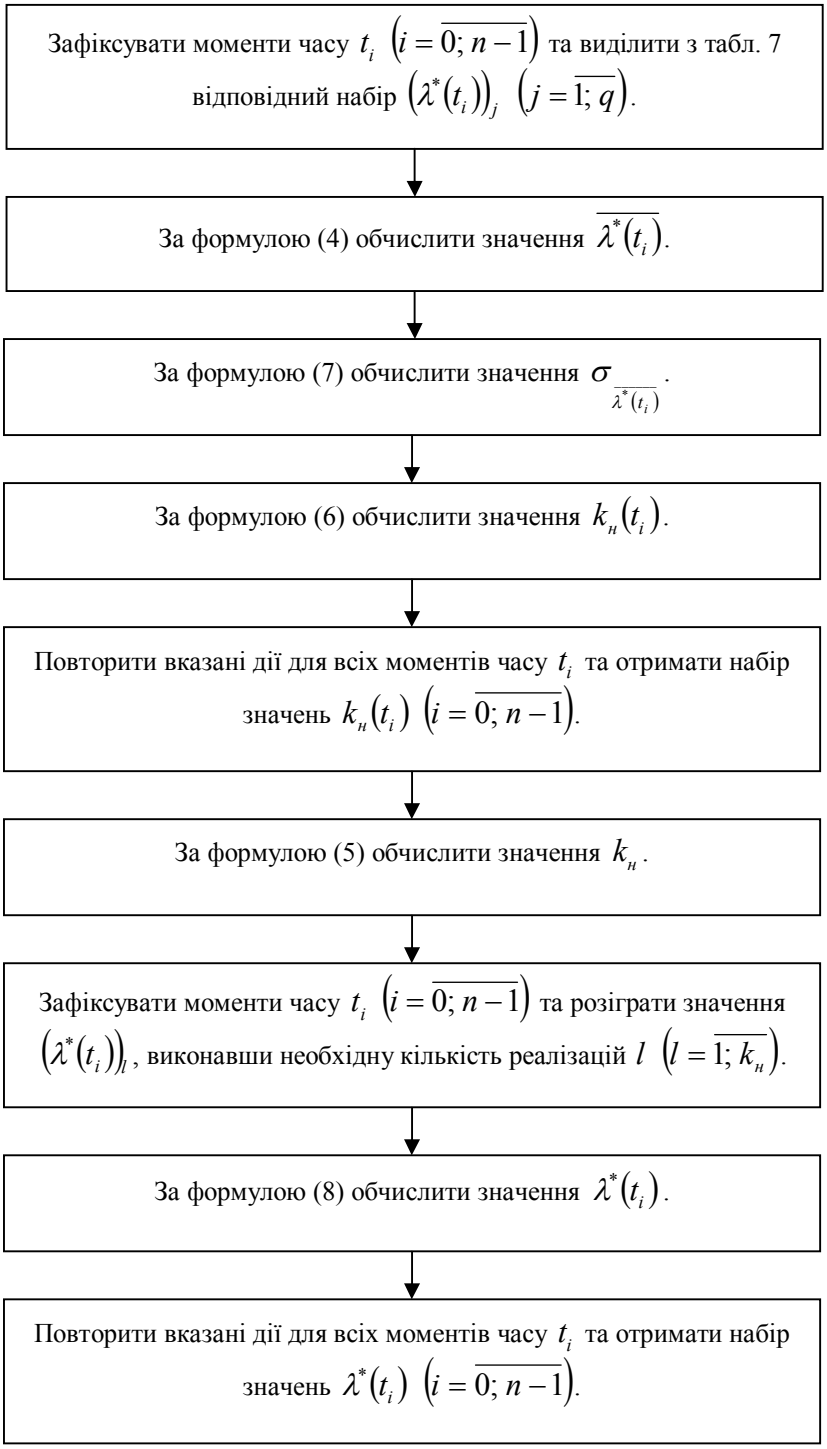

Рис. 4. Схема відшукання значень $\lambda^*(t_i)$

Аналогічно тому, як обґрунтовано процедуру відшукання значень інтенсивностей відмов $\lambda^*(t_i)$, можна обґрунтувати процедуру відшукання інтенсивностей відновлень $\mu^*(t_i)$ досліджуваної сукупності ТС для кожного досліджуваного моменту часу t_i. Ця процедура цілком аналогічна.

Знання ж величин $\lambda^*(t_i)$ і $\mu^*(t_i)$ в певні моменти часу t_i $\left(i=\overline{0;n-1}\right)$ дозволяє отримати функціональні залежності для $\lambda(t)$, $\mu(t)$, які являють собою залежність

інтенсивностей відмов і відновлень для досліджуваної сукупності ТС від часу. Для цього можна, наприклад, скористатися методом найменших квадратів [6].

Висновки

Таким чином, у роботі запропоновано новий підхід до визначення інтенсивностей відмов і відновлень складних технічних систем довільної природи, що базується на застосуванні методів імітаційного моделювання.

Подальші дослідження за даним напрямом можуть стосуватися перевірки достовірності результатів проведеного моделювання, а також моделювання функції готовності $S(t)$ на основі знання величин $\lambda(t)$, $\mu(t)$.

Список літератури

1. Вентцель Е.С. Исследование операций / Е.С. Вентцель. – М.: Советское радио, 1972. – 552 с.
2. Основы надежности и технического обеспечения радиоэлектронных средств РТВ ПВО / под ред. Б.П. Креденцера. – К. : Изд. КВИРТУ ПВО, 1982. – 226 с.
3. Острейковский В.А. Теория надежности [Текст] : учебник для студ. вузов, обучающихся по направлениям «Техника и технологии» и «Технические науки» / В.А. Острейковский. – Изд. 2-е, испр. – М. : Высшая школа, 2008. – 463 с.
4. Боровик О.В. Моделювання показників надійності технічних пристроїв на основі нестаціонарних марківських процесів / О.В. Боровик, І.В. Гащук // Машинознавство. – Львів, 2003. – №11(77). – С. 49-52.
5. Жлуктенко В.І. Теорія ймовірностей і математична статистика : навч.-метод. посібник. Ч. ІІ. Математична статистика / В.І. Жлуктенко, С.І. Наконечний, С.С. Савіна. – К. : КНЕУ, 2001. – 335 с. – ISBN 966-574-265-5.
6. Трасковецька Л.М. Прикладна математика [Текст] : навч. посіб. для студ. вищ. навч. закл. / Л.М. Трасковецька, Г.Я. Стопець. – Хмельницький : [б.в.], 2004. – 136 с.

ОБОСНОВАНИЕ АЛГОРИТМА ОПРЕДЕЛЕНИЯ ЗНАЧЕНИЙ ИНТЕНСИВНОСТЕЙ ОТКАЗОВ И ВОССТАНОВЛЕНИЙ ТЕХНИЧЕСКИХ СИСТЕМ НА ОСНОВАНИИ ПРИМЕНЕНИЯ МЕТОДОВ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

О.В. Боровик[1], Г.Б. Жиров[2], И.В. Гащук[1]

[1] Национальная академия Государственной пограничной службы Украины имени Б. Хмельницкого, ул. Шевченко, 46, Хмельницкий, 29003, Украина
[2] Военный институт Киевского национального университета имени Тараса Шевченко, просп. Глушкова, 2, корпус 8, Киев, 03680, Украина

В работе предложен новый подход к определению интенсивностей отказов и восстановлений сложных технических систем произвольной природы, который основан на применении методов теории вероятностей, математической статистики, имитационного моделирования и аппроксимации функций. Определение интенсивностей отказов и восстановлений в виде функциональных зависимостей позволяет смоделировать функцию готовности.
Ключевые слова: интенсивность отказов, интенсивность восстановлений, техническая система, имитационное моделирование, алгоритм

JUSTIFICATION OF THE ALGORITHM FOR FINDING THE VALUES OF FAILURE RATE AND RENEWAL OF TECHNICAL SYSTEMS ON THE BASIS OF SIMULATION METHODS

Oleg V. Borovik[1], Hennadiy B. Jirov[2], Iryna V.Haschuk[1]

[1] National Academy of the State Frontier Service of Ukraine named after Bogdan Khmelnitskiy, 46 Shevchenko str., Khmelnytskyi, 29003, Ukraine
[2] Military Institute, Taras Shevchenko National University of Kyiv, 2 Glushkova Ave., build. 8, Kyiv, 03680, Ukraine

The paper suggests a new approach to determine the intensity of failures and restorations of complex technical systems of arbitrary nature, based on the application of probability theory, mathematical statistics, simulation and function approximation. Finding failure rates and restorations in the form of functional dependencies allows model the function of readiness.
Keywords: failure rate, the intensity of the updates, technical system simulation, algorithm

УДК 510.67(07)

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 1, pp. 46-57

АНАЛІЗ МЕТОДІВ СКЛАДАННЯ ОПТИМАЛЬНИХ РОЗКЛАДІВ РОБОТИ СКЛАДНИХ СИСТЕМ

М.В. Капустян[1], Л.Т. Пархуць[2], В.О. Хорошко[1]

[1] Державний університет інформаційно-комунікаційних технологій,
вул. Солом'янська, 7, Київ, 03110, Україна; e-mail: professor_va@ukr.net
[2] Національний університет «Львівська політехніка»,
вул. Степана Бандери, 12, Львів, 79013, Україна; e-mail: par7@i.ua

В даній роботі проведений аналіз методів складання оптимальних розкладів роботи складних систем. Були проведені статистичні випробування запропонованих методів, досліджено питання ефективності застосування багатообчислювальних систем.

Ключові слова: складні системи, розклади роботи, ефективність

Вступ

При проектуванні та розробці розкладів роботи складних систем (СС) необхідно враховувати побудову структур інформаційних потоків, які визначаються раціональними факторами: кількісним, топологічним, якісним, часовим. Основним критерієм є максимізація суми відношень ефектів взаємодії локальних систем до затрат. Ця задача є багатокритеріальною задачею оптимізації, і при її вирішенні виникають труднощі, тому пропонується основний критерій подати у вигляді ієрархії локальних критеріїв, а задачу розробки декомпозувати на ряд локальних задач. Основу декомпозиції складає залежність між локальними критеріями оптимізації і факторами, які враховуються.

Основна частина

При вирішенні задачі побудови оптимального розкладу для СС розрізняють двох- і багатообчислювальні засоби забезпечення. Виходячи з цього, Мунс і Коффман запропонували алгоритм утворення розкладу для однорідної двохобчислювальної системи в припущенні, що час, витрачений на переривання, зневажливо малий [1]. Розглядаються розклади наступного класу.

Нехай $S_1,...,S_m$ – розбиття множини вершин графа G, для якого, якщо $x \in S_j$, $y \in S_i$ і x передує y, то $j < i$. Якщо ваги вершин одиничні, то для кожної множини S_i, $i = \overline{1,m}$, легко скласти розклад R_i. При послідовному з'єднанні таких розкладів отримаємо розклад типу SS для графа G.

Теорема 1. Для графа G з довільними вагами вершин t_i та для двох ідентичних обчислювачів СС оптимальним розкладом з перериванням є оптимальний розклад типу SS, побудований для графа G' (G' отримуємо заміною в графі G вершини з вагою t_i ланцюжком t_i вершин з одиничними вагами).

Знайдений алгоритм побудови розбиття в підсумку дає оптимальний розклад з перериваннями для графа G і є базовим.

Подальшим розвитком цього алгоритму є модель обчислювального процесу в СС з двома обчислювачами. Вага кожної вершини орієнтованого ациклічного графа визначає час відповідного завдання, ваги вершин довільні [2]. Цей алгоритм для визначення часу виконання обчислень є настільки загальним, що забезпечує можливість його використання і в багатомашинних і багатопроцесорних СС. Розглянемо роботу алгоритму. Для цього вводяться позначення: $G\langle X,\Gamma,t,x_0\rangle$ – зважений граф, X – множина вершин, Γ – відношення на X, t – функція, яка ставить у відповідність кожній вершині $x\in X$ додатнє число, x_0 – кінцева вершина, для якої $\Gamma(x_0)=\varnothing$, $\varnothing$ – порожня множина.

Граф $G\langle X,\Gamma,t,x_0\rangle$ назвемо ступінню, якщо і тільки якщо він зв'язний, не містить циклів і має одну кінцеву вершину.

Надалі будемо розглядати тільки мережі, в які входять СС, що позначаються S.

Нехай $S=\langle X,\Gamma,t,x_0\rangle$ – довільна, але фіксована мережа; $L'(i),\ i=1,...,n$ – підмножина, що визначається за законом індукції наступним чином:

1) $L'(1)=x_0$;

2) Якщо $x\in Z_i$ і $t(x)=\min_{y\in Z_i}[t(y)]$, то $x\in L'(i)$, де Z_i – підмножина X, така що

$$Z_i=\left\{x\in X\mid x\in\left[X-\bigcup_1^{i-1}L'(j)\right]\wedge\left[\Gamma(x)\subset\bigcup_1^{i-1}L'(j)\right]\right\},$$

тобто Z_i – множина посередніх попередників для вже побудованих множин $L'(j),\ j=1,...,i-1$.

Нехай p натуральне число, таке що $\bigcup_1^p L'(j)=X$. Тоді для $1\le i\le p$ підмножину $L(i)\subset X$, що визначається як $L(i)=L'(p+1-i)$, назвемо *i*-им рівнем мережі.

Нехай $S_i=\langle X_i,\Gamma_i,t_i,x_{0i}\rangle$ і $S=\langle X,\Gamma,t,x_0\rangle$ – довільні, але фіксовані мережі, для яких $X\subset X_i$. Мережа S_i є прямим розширенням мережі $S\ (S\subseteq S_i)$, якщо і тільки якщо існує дві такі вершини s_i і s_i^*, що $s_i\in X\bigcap X_i$ й $s_i^*\in X_i-X$, задовольняє таким умовам:

1) $\Gamma_i(s_i)=s_i^*$ і $\Gamma(s_i)=S_i(s_i^*)$;

2) $t(s_i)=t_i(s_i)+t_i(s_i^*)$;

3) якщо $x\in X$ і $x\ne s_i$, то $\Gamma(x)=\Gamma_i(x)$.

Вершину s_i назвемо сингулярної вершиною мережі S_i по відношенню до мережі S. Якщо S_i містить більше однієї сингулярної вершини, то мережа S_i називається розширенням мережі S. Слід зазначити, що якщо мережа S_i є яким-небудь розширенням S, то остання не є звуженням мережі S_i, і якщо $s_i\ne x_0$, то $x_0=x_{0i}$.

Розглянемо основний крок розширеного алгоритму [2].

Нехай мережа S_0 – модель обчислень, p_0 – число рівнів мережі S_0. На першому кроці проглядаються елементи послідовності

$$L_0(1),...,L_0(n),...,L_0(p_0) \tag{1}$$

рівнів мережі S_0, поки не з'явиться мінімальна множина $M(0,n)$ взаємозалежних вершин мережі S_0, тобто така мінімальна кількість, в якій ніякі дві вершини не з'єднані шляхами.

Якщо множина $M(0,n)$ містить один вузол, то члени послідовності (1) проглядаються до визначення множини $D(0)$ взаємно незалежних вершин з вершинами $M(0,n)$, з яких утворюється множина $M^*(0)$: $M^*(0)=M(0,n)\cup D(0)$. З іншого боку, якщо потужність множини $M^*(0)$ більше 1, приймемо $M^*(0)$ як $M(0,n)$.

Далі утворюється мінімальне розширення S_0^M мережі S_0, в якому всі безпосередні приймачі вершин, що належать $M(0,n)$, містяться в тому ж рівні мережі S_0^M.

Якщо це можливо, утворюється розбиття $\{P(0), M^*(0)-P(0)\}$ множини $M^*(0)$ таким чином, щоб задовольнити відношенню

$$\sum_{x\in P(0)} t_0^M(x)=\frac{1}{2}\sum_{x\in M^*(0)} t_0^M(x). \qquad (2)$$

Якщо таке відношення нереалізоване, то згідно деякому правилу [2] вибираємо завдання з множини завдань, що відповідають множині вершин $M^*(0)$, і розбиваємо на дві частини таким чином, щоб задовольнити рівності (2).

Завдання, відповідні множинам $P(0)$, $M^*(0)-P(0)$, виконуються різними обчислювальними засобами.

Для оптимально розкладу вирішення набору завдань, зв'язаних відношеннями передування, представлених у вигляді орієнтованого зваженого графа без циклів $G=(X,U)$ (X – множина вершин, U – множина ребер, ваги всіх вершин однакові і дорівнюють $t_i=1$, $i=\overline{1,r}$, де $r=[X]$), пропонується алгоритм, для якого число кроків обчислення пропорційну числу дуг графа G. Алгоритм полягає в послідовних кроках розподілу по обчислювачам вершин, найбільш віддалених від кореня дерева [2].

Для багаторубіжної і багатоланкової системи захисту об'єму була вирішена задача складання розкладу з перериванням для однорідної СС, коли граф G є деревом [1]. Обчислювачі розглядаються як загальна обчислювальна потужність СС. Передбачається, що для виконання розрахунку будь-якої вершини графа може бути призначена обчислювальна потужність $a\in[0,1]$. Ця операція відповідає збільшенню часу розширення вершини в $1/a$ разів. Такий тип розкладу називається *GS* (*General Scheduling*).

Теорема 2. Для всіх $G=(X,U)$ і n (n – число обчислювачів) довжина оптимального *GS* розкладу дорівнює довжині оптимального розкладу з перериваннями.

Алгоритм задачі зводиться до призначення n/m частини обчислювальної потужності обчислювача на кожну з m вершин, найбільш віддалених від кореня дерева, якщо $n\le m$, і всього обчислювача, якщо $n>m$. Призначення не розглядаються, коли виконання вершин зводить їх до рівня, на якому є ще призначені вершини.

У [3] вирішується завдання розподілу набору n незалежних задач по m обчислювачам системи $P_1,...,P_m$. При цьому швидкість роботи обчислювача P_i дорівнює S_i і $S_1\ge...\ge S_m$, а час обробки *i*-го завдання дорівнює t_i. Передбачається, що завдання впорядковані так, що $t_1\ge...\ge t_n$, на виконання *i*-го завдання на *j*-му процесорі потрібен час t_i/S_j, $i=\overline{1,n}$, $j=\overline{1,m}$. Під розподілом з оптимальним часом завершення – *OFT* (*Optimal Finish Time*) – розуміють розклад з мінімальним часом завершення серед допустимих розкладів для даних незалежних задач та системи обчислювачів.

Теорема 3. Для будь-якого набору n незалежних задач і будь-якої системи m обчислювачів різної продуктивності ($m\ge1$) існує *OFT* розклад з перериванням, для якого потрібно не більше $2(m-1)$ переривань.

Доказ цього твердження є конструктивним і дає алгоритм отримання розкладу з необхідними властивостями. Тимчасові витрати складають $O(n)$ без урахування часу на сортування завдань та обчислювачів. При необхідності проведення упорядкування вони зростають до $O(n+m\log_2 n)$. У пропонованому алгоритмі на кожному кроці проводиться розбиття множини зайнятих обчислювачів I на $I_1 \bigcup I_2 = I$, де $I_1 = \{P_1,...,P_j\}$, $I_2 = \{P_{l_1},...,P_{l_{k-1}}\}$ такі, що $j+1 \neq l_1$, $l_1 \le l_2 \le ... \le l_{k-j}$, де k – номер чергового завдання ($k < m$). На кожному кроці проводиться формування роздільної системи обчислювачів *DPS* (*Disjoint Processor System*), що є такою множиною обчислювачів $P_{i_1},...,P_{i_r}$, $r \ge 1$, що $i_1 \le i_2 \le ... \le i_r$ і обчислювач P_{i_j} простоює проміжок часу $[U_{j-1},U_j]$, $j = \overline{1,r}$, для деяких $U_0,U_1,...,U_r$, які мають властивості $U_0 = 0$, $U_r = w$, $U_{j-1} < U_j$, $j = \overline{1,m}$. Чергове завдання призначається на обчислювачі, що мають простої і утворюють *DPS*. Якщо цього часу недостатньо, то проводиться призначення на обчислювач $P_j \notin I$ та володіє максимальною швидкодією серед тих, що залишилися. Коли $k = m$, значення $k, k+1,...,i$, де i визначається з нерівності: $\sum_{j=k}^{i} t_j \le w\sum_{j=1}^{i} S_{r_j}$, можуть бути призначені на обчислювачі $P_{r_1},...,P_{r_i}$ з використанням процедури, запропонованої Макнотоном [4] для ідентичних обчислювачів. Обчислювачі призначаються за порядком: P_{r_1} перед P_{r_2}, P_{r_2} – перед P_{r_3} і т.д. Призначення на кожен обчислювач проводиться справа наліво.

Мунц і Янг у роботі [5] отримали наступну оцінку *OFT* розкладу. Нехай w – довжина *OFT* розкладу з перериваннями, $T_j = \sum_{i=1}^{j} t_i$, $S_j = \sum_{i=1}^{j} S_i$ і $n \ge m$, тоді $w \ge \max_{1\le i<n}\left\{\max_{1\le j<m}\left[\frac{T_i}{S_j}\right]\right\}$. Алгоритм Мунтіна і Коффмана [1], використаний для системи обчислювачів з різною продуктивністю, дозволив отримати алгоритм стану *OFT* розкладу з числом переривань $n^2(m-1)$, який вимагає обчислювальних затрат $O(mn^2)$ [6]. Цей алгоритм показує, що довжина w *OFT* розкладу завжди задовольняє рівності $w = \max_{1\le i<n}\left\{\max_{1\le j<m}\left[\frac{T_i}{S_j}\right]\right\}$.

Розглянемо методи отримання оптимальних розкладів без переривань. Для систем з двома обчислювачами запропонований в [7] алгоритм A отримання оптимального розкладу для завдань, представлених у вигляді паралельно-послідовних мереж (ПП-мереж). Послідовність кроків алгоритму відповідає порядку перегляду графа.

ПП-мережа – це граф, одержуваний послідовним застосуванням операцій: паралельного $(\times)$ і послідовного $(+)$ з'єднання, починаючи з мережі, що складається з одного ребра. Передбачається, що ребра розглянутих ПП-мереж відповідають операторам обчислювального процесу і час виконання кожного оператора дорівнює одиниці.

Розглянемо спочатку графи загального вигляду. Нехай задані графи $G_1(X,U)$ і $G_2(Y,V)$, де $X = Y = \Phi_1$, $U = V = \Phi_2$, R_1 і R_2 – оптимальні двохобчислювальні розклади для цих графів. Нехай $R_1 = (a_1,b_1)(a_2,b_2)..(a_n,b_n)$, $R_2 = (c_1,d_1)(c_2,d_2)..(c_m,d_m)$, де a_i, c_j є або символами простою $\varnothing$, або ребрами відповідно з $U_i, V_j, b_i \in U$, $d_j \in V$ $(i = \overline{1,n}, j = \overline{1,m})$. Позначимо число простоїв в R_1 і R_2 через P_1 і P_2. Тоді $\overline{n}_1 = n - P_1$ і $\overline{n}_2 = m - P_2$ – число безпростойних пар в R_1 і R_2 відповідно.

Теорема 4. За розкладами R_1 і R_2, оптимальними для G_1 і G_2, за допомогою алгоритму A можна побудувати розклад R, оптимальний для графа $G_1 \cup G_2 = (X \cup Y, U \cup V)$.

Алгоритм, виконаний на підставі доведення теореми 4, зводиться до заповнення простою з розкладу R_1 елементами з іншого розкладу R_2, причому для цього заповнення використовуються елементи незаповнених пар. Якщо їх не вистачає для заповнення всіх простоїв, то використовуються елементи безпростойних пар.

Ґрунтуючись на теоремі 4, можна рекурсивно визначити оптимальний розклад для ПП-мережі. Позначимо через $R(F)$ оптимальний двохобчислювальний розклад для мережі F.

1) Нехай $F = d$, тобто мережа складається з єдиного ребра. Тоді $R(F) = R(d)$.

2) Нехай $F = F_1 + F_2$ і вже побудовані $R_1(F_1)$, $R_2(F_2)$. Тоді $R(F) = R_1(F_1)R_2(F_2)$ – послідовне з'єднання розкладів.

3) Нехай $F = F_1 \times F_2$ і вже побудовані $R_1(F_1)$, $R_2(F_2)$. Тоді $R(F)$ можна отримати за допомогою алгоритму A.

Ці міркування справедливі і для випадку, коли граф є узагальненою ПП-мережею, вершинами якої є мережі довільного виду, якщо для цих елементарних мереж відомі їх оптимальні двохобчислювальні розклади.

В алгоритмі отримання оптимального двохобчислювального розкладу для довільного графа з рівними вагами вершин [8] на першому етапі виконується побудова максимального парасполучення в графі $\overline{G}$ – додатковому для графа G. Потім знайдене парасполучення послідовно перебудовується в таке максимальне, яке допускало б впорядкування з графом G.

Для систем з довільним числом обчислювачів в [9] запропоновані алгоритми знаходження оптимального розкладу набору n незалежних операторів на неоднорідну обчислювальну систему, що складається з $m = n$ обчислювачів, для випадків кратної і некратної продуктивності обчислювачів з одним завданням на кожен обчислювач.

У першому випадку проводиться впорядкування операторів та обчислювачів за часом рішення і продуктивністю, потім здійснюється призначення більш довгих завдань на більш продуктивні обчислювачі. Нехай, наприклад, матриця T, яка пов'язує r_i, $i = \overline{1,4}$, – час реалізації оператора на еталонному обчислювачі і r_j, $j = \overline{1,4}$ – коефіцієнти кратності продуктивності еталонного обчислювача по відношенню до *k*-го обчислювача, має вигляд:

$$T = \begin{pmatrix} 1 & 3 & 9 & 2 \\ 5 & 15 & 45 & 10 \\ 4 & 12 & 36 & 8 \\ 2 & 6 & 18 & 4 \end{pmatrix}.$$

Впорядкуємо r_i, r_j. Отримаємо:

1_1	2_4	4_3	5_2
9_3	3_2	2_4	1_1

Виходячи з цього, розподіляємо перший оператор на третій обчислювач, другий на перший, третій на четвертий і четвертий на другий. При цьому $T_1 = 9$, $T_2 = 6$, $T_3 = 8$, $T_4 = 5$ і $\max\limits_i T_i = 9$.

У разі некратної продуктивності обчислювачів системи запропоновано ітераційний алгоритм, для якого доведена збіжність до оптимального рішення задачі про призначення.

У роботі [7] розглядається задача про оптимальне призначення завдань на неоднорідних обчислювачах кратної продуктивності, проте в припущенні, що на один обчислювач можна призначити декілька завдань. Алгоритм, який реалізує вибір оптимального призначення, працює наступним чином:

Крок 1. Робиться призначення завдань відповідно до алгоритму для випадку кратної продуктивності [9];

Крок 2. Перевіряється отриманий розклад на оптимальність. Якщо він оптимальний, то алгоритм завершує роботу, інакше проводяться перебори: завдання з повільних обчислювачів перерозподіляються на більш швидкі.

Задача розподілу незалежних завдань часто вирішуються в такій постановці. Нехай система платить штраф P_i за кожну задачу x_i, якщо вона завершується в момент t_i, де t_i визначає час від початку роботи системи над комплексом завдань. Потрібно визначити розклад, який мінімізує загальну суму штрафів. Для однообчислювальної системи оптимальна послідовність призначення завдань виходить при упорядкуванні завдань по незростанню величин P_i/t_i [10].

Нехай C_m – загальний штраф при оптимальному використанні m обчислювачів. Загальний штраф при призначенні на один обчислювач становить:

$$C_1 = P_1 t_1 + P_2(t_2 + t_1) + \ldots + P_n \sum_{i=1}^{n} t_i .$$

Якщо $C_n = \sum_{i=1}^{n} P_i t_i$, тоді $C_m \geq \frac{1}{m} C_1 + \frac{m-1}{2m} C_n$, тобто на обчислювачі, що працює в m разів швидше еталонного, рішення n завдань більш ефективно, ніж на еталонних.

Запропонований в [11] алгоритм призначення завдань на обчислювачі однорідної обчислювальної системи (ООС), заснований на виборі чергового завдання з послідовності завдань, упорядкованих за зростанням t_i/C_i, для призначення на обчислювач, який звільнився.

Для розподілу обчислювачів при багаторазовій обробці набору завдань різної тривалості обробки можна використовувати метод, викладений в [7], в якому оптимальний графік обробки реалізується шляхом вирішення задачі лінійного програмування.

Проблема розподілу завдань з обчислювача обчислювальної системи може бути в принципі вирішена методами математичного програмування [12, 13], проте практичне їх застосування обмежено через велику трудомісткість.

Для отримання оптимального розкладу використовувався також метод гілок і меж [12]. Проаналізована та показана його придатність до завдань, представлених у вигляді графів без циклів з одиничними вагами вершин. Дані про часові витрати на складання розкладу для вибору незалежних завдань з довільним часом рішення для однорідної n-обчислювальної системи відсутні. Однак, судячи з того, що складність цього методу зростає для трьохобчислювальної системи в порівнянні з двохобчислювальною [12] для багатообчислювальних систем його використання є недоцільним.

Метод гілок і меж застосовується для розв'язання задачі оптимального призначення в такій постановці [13]. Є m неоднорідних виконавців і n робіт. Задана матриця часу $\left(t_{ij}\right)_{i=\overline{1,n},\ j=\overline{1,m}}$ виконання i-ї роботи j-м виконавцем. Роботи між виконавцями розподіляються таким чином, щоб кожен з них виконував не більше k робіт і при паралельній роботі виконавців час виконання всіх робіт був мінімальний.

В даний час широко використовуються стохастичні методи розподілу завдань. Їх застосування доцільне в разі багаторазового використання отриманих результатів, оскільки рішення задачі стохастичної оптимізації вимагає значних витрат машинного часу.

У роботі [12] запропоновано алгоритм функціонування обчислювальної системи, що використовує методи теорії ігор. У цьому випадку гравцями є обчислювальний центр і диспетчер. Перший має n ідентичних обчислювачів і використовує стратегію $i \in E$ $\left(E = \{0,1,...,n\}\right)$, якщо для вирішення завдань відводиться i обчислювачів. Завданню присвоюється ранг $j \in E$, коли для вирішення потрібно j обчислювачів. Передбачається, що інтенсивність надходження завдань досить висока, оскільки в будь-який момент часу в системі є завдання різних рангів. Будь-яке завдання рангу $j \in E$ вирішується на обчислювачах за одиницю часу. Це не порушує єдності міркувань, тому що при великій інтенсивності потоку задач від випадку, при якому завдання мають довільні значення часу рішення, легко перейти до випадку, при якому завдання мають одиничні значення часу рішення [12]. Змішана стратегія диспетчера – $\Pi = (\pi_1, \pi_2, \ldots, \pi_n)$, $\sum_{i=1}^{n} \pi_i = 1$, де π_i – імовірність того, що диспетчер направив на обчислювальний центр завдання рангу i. Змішана стратегія обчислювального центру – $P = (P_0, P_1, \ldots, P_n)$, $\sum_{i=0}^{n} P_i = 1$, де P_i – імовірність того, що обчислювальний центр використовує i обчислювачів для вирішення завдань. Для цього вводиться матриця платежів диспетчера обчислювальному центру $C = (c_{ij})$, де c_{ij} – платіж диспетчера обчислювальному центру за умови, що обчислювальний центр вибрав стратегію i, а диспетчер стратегію j. Методами теорії ігор знаходиться оптимальна змішана стратегія P^* обчислювального центру та диспетчера Π^*: $V = P^* C \Pi^*$, або $V = \max_P \min_\Pi PC\Pi = \min_\Pi \max_P PC\Pi$.

Пару (P^*, Π^*) називаємо рішенням ігрової задачі, а V – ціною. Трудомісткість визначення змішаних стратегій P^* і Π^* не є перешкодою на шляху використання даного підходу, оскільки для заданих систем і платіжної матриці потрібно знайти рішення тільки один раз.

У [12] було запропоновано метод стохастично-оптимального розподілу обчислювачів по терміналах, який враховує попит на підсистеми різних рангів з терміналів для розподілених ООС різних конфігурацій. При цьому передбачається, що на термінали надходять завдання різних рангів, а попит на підсистеми різних рангів підпорядкований закону Пуассона. Задача оптимального розподілу зводиться до задачі стохастичного програмування, яку неможливо вирішити. Тому був застосований метод ланцюгів Монте-Карло і показана його придатність для вирішення подібних завдань.

У [14] розроблено алгоритм диспетчеризації для обчислювального процесу, заданого стохастичною граф-моделлю. Для опису ходу обчислювального процесу застосовується апарат однорідних ланцюгів Марісова, що дозволяє отримати математичне очікування часу виконання програми. Алгоритм диспетчерування на кожному кроці призначення вибирає активним такий сегмент програми з числа тих, що очікують, що математичне очікування часу, який залишається для закінчення програми, буде не менше, ніж при виборі будь-якого іншого сегмента, що очікує. Запропонований алгоритм диспетчерування доцільно застосовувати в тих випадках, коли витрати часу обробки на обчислювачі на власне диспетчерування є мінімальними, а при створенні програм виправдані роботи з їх аналізу та визначенню ваг і пріоритетів. Це стосується насамперед програм управління обчислювальними системами і програм багаторазового застосування.

Вперше евристичний алгоритм складання розкладу в багатообчислювальній системі був запропонований Ю.С. Шварцем для розподілу інформативно-звя'зкових вершин, представлених у вигляді графа G без розгалужень і циклів, коли вершина може виконуватися на обчислювачі тільки одного типу [14].

Для графа G будується матриця розподілу A, що містить всю інформацію, необхідну для складання розкладу – умови чергування і час виконання для кожної вершини. Визначення підмножини розподілених вершин проводиться за такими евристичними правилами:

1) Розподіл вершин проводиться з мінімізацією простоїв;

2) У першу чергу виконуються вершини з великим числом передування;

3) Серед вершин з однаковим числом передування пріоритет мають оператори з меншим часом виконання.

Алгоритм гарантує допустимість рішень, що задовольняють всім вимогам черговості. Після кожного розподілу проводиться переформування матриці відповідно до деяких евристичних правил.

Алгоритм, запропонований в [15], був розвинений для однорідної двохобчислювальної системи в припущенні, що кожна вершина може виконуватися на будь-якому обчислювачі за одиницю часу. Розподіляються оператори, представлені у вигляді орієнтовного зваженого графа без контурів. Визначаються оператори, що не мають попередників, і призначаються на обчислювачі; матриця інциденцій графа переформовується з урахуванням того, що деякі вершини вже призначені (останні виключаються з розгляду); в матриці інциденцій шукаються сторони з нульовими елементами, і вершини, відповідні цим сторонам, призначаються на обчислювачі відразу ж або після простою в обчислювачі, щоб значення часу зайнятості обчислювачів відрізнялося як можна менше, тобто оператори пропускаються єдиним фронтом. Алгоритм Шварца застосовували так само в припущенні, що кожна вершина може бути на обчислювачах різних типів.

Подальшим розвитком цього напряму є обліковий алгоритм отримання розкладу [16], який застосовується до розподілу вершин графа G за однорідними обчислювачами. Вивчаючи ефективність списочних алгоритмів [16] розподілу завдань, запропонованих раніше алгоритмів [1], можна зробити висновок, що для обчислювальних систем побудований з їх допомогою розклад у гіршому разі вдвічі довше оптимального.

Розподіл вершин графа за обчислювачами може здійснюватися за допомогою ярусно-паралельної форми графа, тобто розбиття множини X вершин графа G: $X = X_1 \cup X_2 \cup ... \cup X_r$. Усі вершини $x \in X_i$ лежать на відстані $i-1$ від входу G [7].

Представлення алгоритмів у ярусно-паралельній формі дозволило розробити ефективні методи отримання розкладів, досить близьких до оптимальних [17]. Це досягається тим, що замість $\min\left(\max_j T_j\right)$, який дає оптимум, але вимагає великого часу розрахунку, шукається $\min \sum_{j=1}^{n} T_j^S$, де S вибирається з умови: $S > \dfrac{\lg r}{\lg\left(\max t_{ij}\right) - \lg a}$, а $T_j = \sum_{i=1}^{m} t_{ij} x_{ij}$, t_{ij} – час вирішення i-ї вершини на j-му обчислювачі, $i = \overline{1,m}$, $j = \overline{1,n}$, $a = \max_{i,j} t_{ij}$

$$x_{ij} = \begin{cases} 1, \text{ якщо } i-\text{й алгоритм розподілено на } j-\text{й обчислювач;} \\ 0, \text{ інакше} \end{cases}.$$

Необхідним є виконання наступних умов: $\sum_{i=1}^{m} x_{ij} \le k$, $\sum_{j=1}^{n} x_{ij} = 1$.

Інший майже оптимальний алгоритм побудови розкладів без переривань для дерева з довільними вагами вершин полягає у призначенні на вільний обчислювач вершини, найбільш віддаленої від кореня дерева [16].

У [18] пропонується евристичний алгоритм розподілу ресурсів. Передбачається, що є комплекс, що складається з n операцій, які можна виконувати за мінімально можливий час на обмежених ресурсах. Комплекс операцій представлений у вигляді графа без циклів. Множина операцій розбита на k класів. Для кожного класу задана кількість ресурсів N_j $\left(j=\overline{1,k}\right)$, призначених для виконання операцій даного класу.

Нехай $F(t)$ – множина операцій, які можна виконати (або вони виконуються) у момент t. Ця множина називається фронтом операцій; $R(t)$ – множина номерів цих операцій. У даний момент ресурси розподіляються тільки на роботи фронту. Вибір деякого розподілу відповідає вибору підмножини рішень (множина всіх варіантів розподілу в момент t визначає процес розгалуження). Функція оцінки $\varphi=\sum_{i\in R(t)}\Delta r_i(t)u_i(t)$, де $\Delta r_i(t)$ – повний резерв часу операцій $A_j\in F(t)$; $u_i(t)$ – кількість ресурсів на i операції в момент t. Правило виконання операцій з меншими значеннями $\Delta r_i(t)$ в першу чергу відповідає вибору розв'язку з мінімальним значенням функції оцінки φ.

Метод гілок і меж використаний так само як евристичний алгоритм побудови розкладів для зваженого графа без контурів. Основний евристичний принцип – негайне призначення на звільнившийся обчислювач, якщо є готова до виконання вершина [19].

У [12] запропоновано алгоритм функціонування однорідних універсальних обчислювальних систем у найпростішому випадку, який заснований на переборі заданого числа послідовностей із L завдань і побудові для кожної з них розкладу шляхом послідовного призначення завдань на обчислювачі до тих пір, поки чергове завдання не перевищить на кожному обчислювачі нижню межу часу T

$$T\geq\theta=\frac{1}{n}\sum_{i=1}^{L}t_i\,.$$

Цей алгоритм дає субоптимальний час вирішення набору завдань на обчислювачах системи. Більш швидка відповідність досягається вирішенням питань призначення на j обчислювач з надлишком або недоліком з допомогою методу динамічного програмування [11].

Для розподілу скінченної множини різної швидкості завдань з обчислювача ООС пропонуються два алгоритми [11]. В першому з них множина всіх завдань розбивається на підмножини з завдань, сумарний час вирішення яких близький до θ. Виконання цієї процедури здійснюється за допомогою алгоритму побудови укрупнених задач (підмножин) у припущенні, що штраф за затримку рішення будь-якої задачі дорівнює нулю. У цьому випадку алгоритм розподілу подібний алгоритму формування пакету укрупнених задач, і рішення задачі розподілу проводиться методом ланцюгів Монте-Карло. У другому алгоритмі штраф за затримку виконання завдання відмінний від нуля. У його основу покладений принцип призначення на крок z укрупнених задач, які не призначалися на попередніх кроках $z^*<z$ і сума рангів яких не більше n.

Запропоновані алгоритми дають субоптимальне рішення поставленої задачі розподілу, однак результати статистичних випробувань показали достатню близькість отриманих рішень до оптимальних.

Алгоритм призначення n незалежних робіт на M ідентичних обчислювачах пропонується в роботі [20]. Кожна робота i характеризується часом обробки t_i, штрафом на одиницю часу p_i і директивним терміном $d_i=t_i$ для всіх i. Мета роботи –

мінімізувати загальний штраф $C=\sum_{i=1}^{n} p_i(T_i-t_i)$, де T_i – дійсний час виконання i роботи. Запропонований алгоритм є різновидом методу гілок і меж Ельмахрабі і Паріка [21], в якому відносини передування будуються на основі наступних результатів.

Лема 1. Для $i<j$, якщо $t_i \le t_j$ і $p_i \ge p_j$, робота i передує роботі j $(i<j)$ в оптимальному розкладі.

Передбачається, що робота заздалегідь впорядкована за зростанням $r_i = t_i / p_i$. Якщо $r_i = r_j$, то роботі з меншим часом присвоюється менший номер, якщо $p_i = p_j$ і $t_i = t_j$, то номери присвоюються довільно.

Лема 2. Існує оптимальний розклад, в якій робота 1 призначається першою.

Правило розгалуження в алгоритмі полягає в тому, що призначається завдання з мінімальним номером з множини $A[P(k)]$ на перший обчислювач, який звільнився, конфлікти вирішуються призначенням на обчислювач з меншим номером (тут під $A[P(k)]$ розуміється множина завдань, які можна призначити на позицію $k+1$).

У [18] пропонуються для диспетчерування завдань в ООС два алгоритми. Вони не забезпечують глобальний мінімум величини T – часу рішення задач у системі, але є простими і високоефективними. У першому алгоритмі впорядковані за зростанням часу обробки завдання призначаються на обчислення пачками, починаючи з наступних таким чином, що завдання з великим часом потрапляє на обчислювач з меншим завантаженням. Обчислювачі, завантаження яких рангу $\theta = \frac{1}{n}\sum_{i=1}^{L} t_i$ виключаються з розгляду. Другий алгоритм відрізняється послідовним призначенням завдань з максимальним часом на обчислювачі, які звільняються. Інші алгоритми роботи диспетчера придатні як для однорідної, так і для неоднорідної обчислювальної системи. В основу одного з них покладені наступні правила: при відомих поточних значеннях часу зайнятості обчислювачів в першу чергу пропонуються оператори з великим часом рахунку; оператор призначається на обчислювач, який швидше його закінчить [11]. Запропоновані алгоритми диспетчеризації потоків задач у мережах обчислювальних засобів дозволяють за короткий час будувати розклад, близький до оптимального по деякому критерію якості. Наведений алгоритм отримання оптимальних розкладів заснований на твердженні: якщо черга, упорядкована по відношенню $r_1/t_{1j_0} \ge r_2/t_{2j_0} \ge \ldots \ge r_n/t_{nj_0}$ не містить істотних нулів, то вона оптимальна в сенсі критерію $\sum_{i=1}^{n} r_i \max\{OV[T_i^k(\sigma^0) - T_i^{gup}]\}$, де $T_i^k(\sigma^0)$ – момент часу отримання завдання q_i відповідно до розкладу σ^0; T_i^{gup} – директивний рядок отримання рішення задачі q_i; t_{ij} – час виконання завдання q_i на j-му засобі; r_i – штраф за запізнення рішень завдання q_i щодо директивного рядка T_i^{gup} на одиницю часу. Завдання q_{i^*} з черги називається істотним нулем, якщо $\sum_{f=1}^{i} t_{fj_0} - T_{i^*}^{gup} \langle 0 \text{ и } i \rangle i^*$ таке, що $\sum_{f=1}^{i} t_{fj_0} - T_{i^*}^{gup} > 0$.

Запропоновані алгоритми дозволяють розробляти диспетчерування як планових, так і оперативних завдань. Основна перевага розроблених алгоритмів – мінімальні витрати машинного часу при складанні розкладів.

У [22] розроблені евристичні алгоритми розподілу незалежних завдань на неоднорідні обчислювачі і дано аналіз їхньої поведінки в найгірших умовах.

У [23] запропоновано ітераційний алгоритм отримання розкладу, близького до оптимального в сенсі мінімізації часу завершення, для n незалежних простих завдань по m однорідних обчислювачах. Цей алгоритм у гіршому випадку дає розклад, який перевищує оптимальні за часом 1.2 рази, в той час як алгоритм LPT – в 1.33 рази. Алгоритм, заснований на зведенні задачі розподілу до задачі заповнення бункерів (*Bins*) завданнями, і працює наступним чином:

- задається верхня C_V і нижня C_L межі часу завершення виконання завдання;
- підраховується число обчислювачів, необхідних для виконання завдань за заданий час $C = (C_V + C_L)/2$. Якщо це число $m' > m$, то C береться в якості нової нижньої межі C_L; інакше $C_V = C$.

Такий процес досить швидко сходиться до часу рішення, близькому до оптимального. Експериментальна перевірка роботи алгоритму показала, що отриманий розклад при $k = 7$ ітераціях перевищував оптимальний час не більше, ніж в 1.024 рази. Слід зазначити, що при використанні запропонованого алгоритму потрібно $\underline{O}(n \log n + kn \log m)$ кроків, тобто більше, ніж для алгоритму LPT, однак при цілком прийнятних втратах в часі досягається велика точність обчислень.

Висновки

Були проведені статистичні випробування запропонованих точних і евристичних методів диспетчерування. Досліджені питання статистичної ефективності застосування багатообчислювальних систем, складності та точності методів, аномалії складності і точності. Обчислювальний процес моделювався графом без контурів. Розглядались потоки обчислювального процесу, які характеризуються фіксованим числом операторів і кількісним розподілом. Ваги всіх вершин покладаються рівними одиниці. Аномалії вивчалися шляхом застосування алгоритмів і графів обчислювальних процесів в різних записах з подальшим порівнянням результатів. При дослідженні деякого метода M для потоку $k(n, p)$ (p – ймовірність появи одиниці в матриці суміжності для графа обчислювального процесу) по відношенню до обчислювальної системи, яка складається із m однорідних обчислювачів, визначалися наступні характеристики.

Список літератури

1. Muntz R.R. Optimal Preemptive Scheduling on Two-Processor Systems / R.R. Muntz, E.G. Coffman // IEEE Transactions on Computers. – 1969. – Vol.18, Iss.11. – PP. 1014-1020.
2. Rowicki A. A note on optimal preemptive scheduling for two processor systems // Information Processing Letters. – 1977. – Vol.6, Iss.1. – PP. 25-28.
3. Gonzalez T. Preemptive scheduling of uniform processor systems /T. Gonzalez, S. Sahni // Journal of the ACM. – 1998. – Vol.25, Iss.1. – PP. 92-101.
4. McNaughton R. Scheduling with Deadlines and Loss Functions // Management Science. – 1959. – Vol.6, No.1. – PP. 1-12.
5. Liu J.W.S. Optimal scheduling of independent tasks on heterogeneous computing systems / J.W.S. Liu, A.T. Yang // Proceedings of the ACM National Conference. – ACM, 1974. – Vol.1. – PP. 38-45.
6. Horvath E.C. A Level Algorithm for Preemptive / E.C. Horvath, S. Lam, R. Sethi // Journal of the ACM. – 1977. – Vol.24, Iss.1. – PP. 32-43.
7. Олешко Т.И. Оптимальное размещение пунктов обслуживания в сетях / Т.И. Олешко, В.А. Кудинов, В.А. Хорошко // Всеукраинский межведомственный научно-технический сборник «Радиотехника». – ХНУРЭ, 2004. – Вын.139. – С. 151-157.
8. Fujii M. Optimal Sequencing of Two Equivalent Processors / M. Fujii, T. Kasami, K. Ninomiya // SIAM Journal on Applied Mathematics. – 1969. – Vol.17, Iss.4. – PP. 784-789.
9. Томашевський В.М. Моделювання систем : підруч. для студ. вищ. навч. закл. / В.М. Томашевський. – К. : Видавнича група BHV, 2007. – 349 с.

10. Eastman W.L. Bounds for the Optimal Scheduling of *n* Jobs on *m* Processors / W.L. Eastman, S. Even, I.M. Isaacs // Management Science. – 1964. – Vol.11, No.2. – PP. 268-279.
11. Kunde M. First fit decreasing scheduling on uniform multiprocessors / M. Kunde, H. Steppat // Discrete Applied Mathematics. – 1985. – Vol.10, Iss.2. – PP. 165-177.
12. Евреинов Э.В. Однородные вычислительные системы / Э.В. Евреинов, В.Г. Хорошевский. – Новосибирск: Наука, 1978. – 319 с.
13. Айдинян А.Р. Генетические алгоритмы распределения работ / А.Р. Айдинян, О.Л. Цветкова // Вестник ДГТУ. – 2011. – Т.11, №5 (56). – С. 723-729.
14. Сирченко Г.А. Имитационные моделирования для исследования информационных потоков в системе связи / Г.А. Сирченко, В.А. Хорошко // Сучасний захист інформації. – 2010. – №1. – С. 73-77.
15. Szwarc W. Solution of the single machine total tardiness problem / W. Szwarc, F.D. Croce, A. Grosso // Journal of Scheduling. – 1999. – Vol.2, Iss.2. – PP. 55-71.
16. Coffman E.G. A Survey of Mathematical Results in Flow-Time Scheduling for Computer Systems // Lecture Notes in Computer Science. – 1973. – Vol.1. – PP. 25-46.
17. Кудинов В.А. Оптимизация структуры информационной сети / В.А. Кудинов, Л.Т. Пархуць, В.А. Хорошко // Захист інформації. – 2004. – №3. – С. 44-49.
18. Деммель Д. Вычислительная линейная алгебра [Текст] : теория и приложения / Д. Деммель; Пер. с англ. Х.Д. Икрамова. – М. : Мир, 2001. – 430 с.
19. Ramamoorthy C.V. Optimal Scheduling Strategies in a Multiprocessor System / C.V. Ramamoorthy, K.M. Chandy, M.J. Gonzalez // IEEE Transactions on Computers. – 1972. – Vol.21, Iss.2. – PP. 137-146.
20. Wesley Barnes J. An Improved Algorithm for Scheduling Jobs on Identical Machines / J. Wesley Barnes, J.J. Brennan // AIIE Transactions. – 1977. – Vol.9, Iss.1. – PP. 25-31.
21. Elmaghraby S.E. Scheduling Jobs on a Number of Identical Machines / S.E. Elmaghraby, S.H. Park // AIIE Transactions. – 1974. – Vol.6, Iss.1. – PP. 1-13.
22. Ibarra O.H. Heuristic Algorithms for Scheduling Independent Tasks on Nonidentical Processors / O.H. Ibarra, C.E. Kim // Journal of the ACM. – 1977. – Vol.24, Iss.2. – PP. 280-289.
23. Coffman E.G. An Application of Bin-Packing to Multiprocessor Scheduling / E.G. Coffman, M.R. Garey, D.S. Johnson // SIAM Journal on Computing. – 1978. – Vol.7, Iss.1. – PP. 1-17.

АНАЛИЗ МЕТОДОВ СОСТАВЛЕНИЯ ОПТИМАЛЬНОГО РАСПИСАНИЯ РАБОТЫ СЛОЖНЫХ СИСТЕМ

М.В. Капустян[1], Л.Т. Пархуць[2], В.А. Хорошко[1]

[1] Государственный университет информационно-коммуникационных технологий,
ул. Соломенская, 7, Киев, 03110, Украина; e-mail: professor_va@ukr.net
[2] Национальный университет «Львовская политехника»,
ул. Степана Бандеры, 12, Львов, 79013, Украина; e-mail: par7@i.ua

В данной работе проведен анализ методов составления оптимальных расписаний работы сложных систем. Были проведены статистические испытания предложенных методов, исследован вопрос эффективности использования многовычислительных систем.

Ключевые слова: сложные системы, расписание работы, эффективность

ANALYSIS OF THE METHODS FOR OPTIMAL SCHEDULING OF COMPLEX SYSTEMS

Maria V. Kapustyan[1], Lubomyr T. Parhuts[2], Volodymyr O. Khoroshko[1]

[1] State University of Information and Communication Technologies,
7 Solomenskaya str., Kyiv, 03110, Ukraine; e-mail: professor_va@ukr.net
[2] Lviv Polytechnic National University,
12 St. Bandera str., Lviv, 79013, Ukraine; e-mail: par7@i.ua

In this paper the analysis of the methods for optimal scheduling of complex systems has been made. The statistical tests of the proposed methods and the efficiency of multicomputing systems were conducted.

Keywords: complex systems, schedule, efficiency

УДК 681.322

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 1, pp. 58-63

ПРИСТРІЙ РЕГУЛЮВАННЯ ЗМІННОЇ НАПРУГИ З СИСТЕМОЮ АВТОМАТИЧНОГО РЕГУЛЮВАННЯ, ЩО ПЕРЕБУДОВУЄТЬСЯ

Ю.О. Гунченко[1], О.В. Сєлюков[2], К.Ф. Боряк[3]

[1] Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: 7996445@mail.ru
[2] ДП «Науковий центр точного машинобудування»,
вул. Бориспільська, 9, Київ, 02099, Україна
[3] Одеська державна академія технічного регулювання та якості,
вул. Ковальська, 15, Одеса, 65020, Україна

Проаналізовано типи та принципи побудови сучасних регуляторів змінної напруги – стабілізаторів. Запропоновано систему автоматичного управління (САУ) для пристроїв, що розглядаються, з перебудованою в залежності від похибки регулювання структурою. Приведені діаграми роботи для системи імпульсно-фазової модуляції. Отримано передавальні функції САУ, які дійсні для різних способів регулювання. Запропонована система дозволила поліпшити основні показники якості регуляторів напруги – час встановлення, перерегулювання, стала похибка.

Ключові слова: зміна напруга, стабілізатор, система імпульсно-фазового регулювання (СІФУ), система автоматичного управління (САУ), передаточна функція

Постановка проблеми

Пристрої регулювання змінної мережної напруги – стабілізатори – все ширше використовуються у системах електропостачання промислових та побутових споживачів [1].

Якість їх функціонування залежить не тільки від принципу побудови виконавчого органу (ВО), забезпечення необхідної кількості ступенів перетворення та безпечності режимів функціонування, але й в значний мірі від системи управління.

Аналіз останніх досліджень і публікацій

На сьогодення найбільш поширеними типами стабілізаторів змінної мережної напруги є [1, 2]:

- стабілізатори релейного типу з дискретним шагом зміни вихідної напруги;
- стабілізатори плавного типу з безперервною (плавною) зміною вихідної напруги.

Перші частіше будуються по автотрансформаторній (АТ) схемі виконуючого органу (ВО), вихідна напруга яких регулюється перемиканням відводів АТ.

Другі будуються з АТ, вольтододатковим (ВД) або електромеханічним ВО [2, 3].

У будь якому випадку величина напруги змінного струму є інтегральною величиною

$$U = \sqrt{\frac{1}{T}\int_0^T u^2(t)dt}\ ; \quad U_{ср} = \frac{1}{T}\int_0^T |u(t)|dt\ ,$$

де

U – середнє квадратичне або діюче значення напруги;

$U_{ср}$ – середнє значення напруги;

$u(t)$ – миттєве значення напруги;

T – період напруги змінного струму.

Середнє квадратичне значення у найбільшої степені характеризує дію напруги. Більшість пристроїв оперує з середнім значенням, яке простіше вимірювати, і яке, при невеликих спотворюваннях синусоїдальної напруги, за допомогою типових коефіцієнтів просто перераховується у діюче значення. Ці величини розраховуються зазвичай за час, кратний півперіоду $T/2$ і мають дискретний характер, що потребує розглядати систему управління у дискретному вигляді.

Стабілізатори релейного типу ефективно усувають відхилення, не вносять перешкод та завад, але не можуть усунути коливання (скачки) мережної змінної напруги.

Стабілізатори з плавним регулюванням дозволяють з будь-якою заданою точністю підтримувати вихідну напругу та усувають як відхилення, так й коливання мережної змінної напруги.

Виділення невирішених раніше частин загальної проблеми

У публікаціях [1-3] наведено розв’язання технічних проблем побудови виконавчих органів й особливості систем управління перетворювачами змінної напруги, що запобігають аварійним та некоректним станам, що підвищує їх надійність. У [4, 5] наведено приклади побудови та математичний опис систем управління стабілізатором напруги змінного струму. Але в цих публікаціях не враховується й, відповідно, не усувається вплив нелінійності передавальної характеристики ВО, що суттєво впливає на якість регулювання.

Мета статті і постановка досліджень

Метою статті є побудова, опис, та моделювання системи управління регулятором напруги змінного струму – стабілізатора, яка усуває вплив нелінійності силової частини – виконавчого органу й поліпшує якість функціонування пристрою.

Виклад основного матеріалу дослідження

Найбільш розповсюдженим принципом регулювання вихідної напруги є система імпульсно-фазового управління (СІФУ) за допомогою силових ключів – тиристорів, або симисторів. Принцип такого управління полягає у почерговому (один раз у півперіод) включенні пари силових ключів, які виконують під’єднання до виходу сусідніх відводів АТ або ВДТ (рис. 1). Вихідна напруга при цьому регулюється кутом управління α – часом включення наступного (по рисунку з більшим номером) ключа.

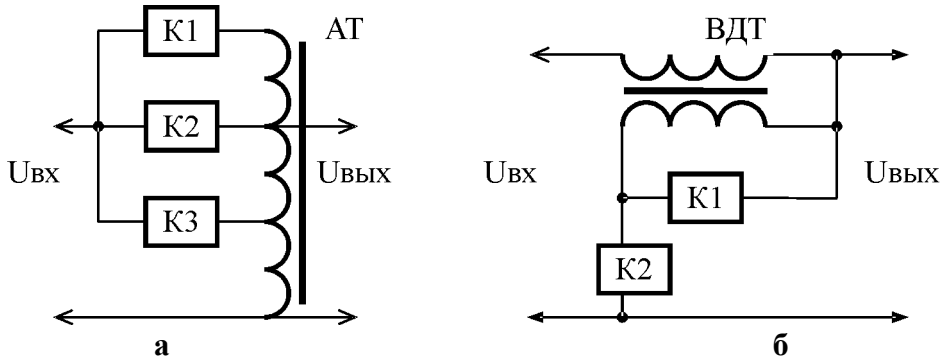

Рис. 1. Функціональні схеми виконуючих органів: а – з автотрансформатором; б – з вольтододатковим трансформатором

Вихідна напруга при СІФУ має вигляд, представлений на рисунку 2, де α – кут управління, φ – кут відставання струму від напругу. Як видно з приведеної осцилограми – нелінійність такого ВО дуже велика, фактично, описується синусоїдальною залежністю добутку прирощення напруги к прирощенню кута управління $du \cdot d\alpha$.

Кут φ залежить від характеру й потужності навантаження й дорівнює куту відставання фази струму від напруги. Він практично не передбачений в процесі функціонування стабілізатора й, також, вносить додаткову нелінійність.

Таким чином, при побудові системи автоматичного управління (САУ) стабілізатором змінної напруги з СІФУ для якісного регулювання необхідно врахувати приведені типи нелінійності.

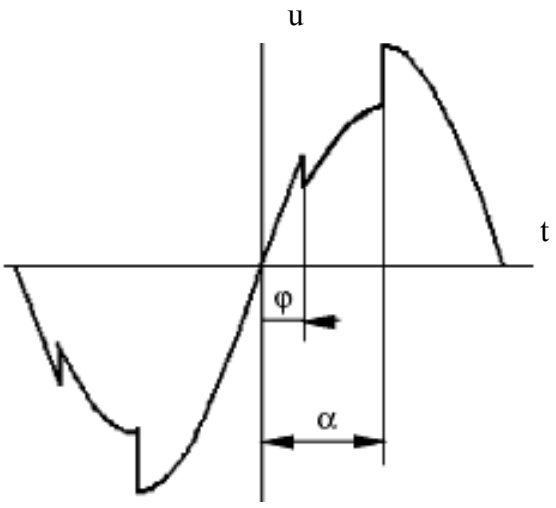

Рис. 2. Вихідна напруга стабілізатора при системі імпульсно-фазового управління

При усереднені передавальної характеристики спостерігаються значні зміни коефіцієнтів передавальної функції САУ, що приводить до непередбаченого характеру перехідних процесів при великих коефіцієнтах підсилення, або до значного збільшення їх часу при малих коефіцієнтах підсилення [4-6].

Усунути вказані недоліки пропонується за рахунок синтезу САУ з структурою, що перебудовується в залежності від величини похибки u (рис. 3).

При малих відхиленнях вихідної напруги $U_{вых}$, коли модуль похибки $|u|$ не перевищує деякого встановленого значення $U_{ош}$ – система функціонує як пропорційно-інтегральна (ПІ) САУ з невеликим коефіцієнтом підсилення K_1. Цей коефіцієнт обирається із умови наявності монотонного перехідного процесу при будь-якому куті управління α. Наявність інтегральної складової дозволяє отримати нульову похибку $u = 0$ у сталому режимі.

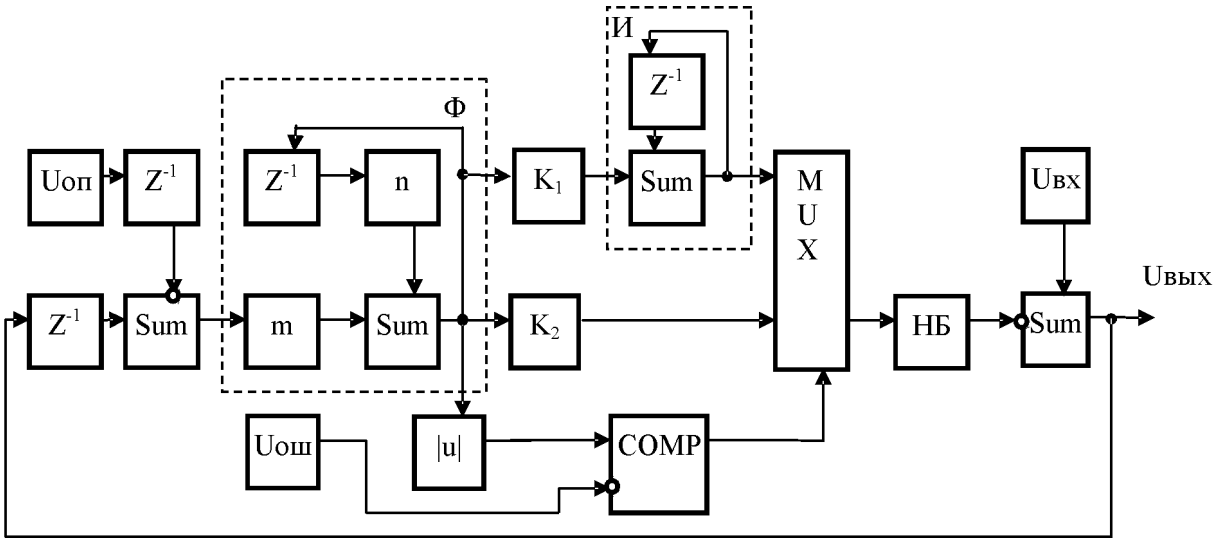

Рис. 3. Функціональна схема САУ стабілізатором з СІФУ: Ф – фільтр низьких частот з коефіцієнтами m и n; $И$ – інтегратор; K_1, K_2 – пропорційні блоки; MUX – мультиплексор; $|u|$ – нелінійний блок – модуль (випрямляч) сигналу; $U_{оп}$ – опорна напруга (дія, що задає), $U_{ош}$ – блок завдання порога зміни структури, $COMP$ – компаратор, $НБ$ – нелінійний блок, $U_{вх}$ – вхідна напруга первинного джерела

При більших відхиленнях вихідної напруги $U_{вых}$ – модуль похибки $|u| > U_{ош}$ перевищує встановлене значення – система функціонує як пропорційна (П) САУ з великим коефіцієнтом підсилення K_2. Цей коефіцієнт обирається із умови формування коливального перехідного процесу, з можливою наявністю перерегулювання, а при кутах регулювання α близьких до $\pi/2$ така САУ може бути нестійкою.

Передавальні функції синтезованої САУ по дії, що збурює $U_{вх}$ та дії, що задає $U_{оп}$ для двох структур (ПІ та П) отримано у наступному вигляді.

Для $|u| < U_{ош}$

$$H(U_{вх}) = \frac{1-(1+n)z^{-1}+nz^{-2}}{1-(1+n-mK_1H_{НБ})z^{-1}+nz^{-2}},$$

$$H(U_{оп}) = mK_1H_{НБ}\frac{z^{-1}-(1+n)z^{-2}+nz^{-3}}{1-(1+n-mK_1H_{НБ})z^{-1}+nz^{-2}}.$$

Для $|u| > U_{ош}$

$$H(U_{вх}) = \frac{1 - nz^{-1}}{1 + (mK_2H_{НБ} - n)z^{-1}},$$

$$H(U_{оп}) = \frac{mK_2H_{НБ}z^{-1}}{1 + (mK_2H_{НБ} - n)z^{-1}};$$

де

$z^{-1} = e^{-p\tau}$ – елементарна затримка;

$\tau = T/2$ – тривалість півперіоду мережної змінної напруги.

Висновки

Моделювання реакцій на стандартні дії показали високу якість перехідних характеристик синтезованої САУ, які володіють малим часом встановлення ($T_S < 4\tau$, по критерію 2%), незначним перерегулюванням ($M_p < 6\%$) й нульової сталою похибкою ($u = 0$) при ступінчатому вхідному збуренню.

Дослідження опитних зразків стабілізаторів змінної напруги, сумісно з синтезованою САУ підтвердило результати моделювання.

Список літератури

1. Грабко В.В. Система автоматичного керування трансформаторами з поздовжньо-поперечним регулюванням під навантаженням / В.В. Грабко, С.М. Левицький. – Вінниця: ВНТУ, 2010. – 119 с.
2. Гунченко Ю.А. Регуляторы переменного напряжения с одним ключевым элементом / Ю.А. Гунченко // Технология и конструирование в электронной аппаратуре. – 1999. – № 5-6. – С. 37-40.
3. Метод безпечної комутації вольтододаткового трансформатора / Ю.О. Гунченко, С.В. Лєнков, М.І. Науменко, О.В. Сєлюков // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка / Київський національний університет імені Тараса Шевченка. Військовий інститут. – Київ, 2009. – Вип. 20. – С. 39-44.
4. Коротецкий Ю.Л. Универсальная модель системы автоматического регулирования переменного напряжения / Ю.Л. Коротецкий, Ю.А. Гунченко // Технічна електродинаміка. Тематичний випуск «Силова електроніка і енергоефективність». – 2000. – Ч. 2. – С. 75-78.
5. Математична модель системи автоматичного регулювання перетворювачем електроенергії / С.В. Лєнков, В.А. Мокрицький, Ю.О. Гунченко, О.В. Банзак // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка / Київський національний університет імені Тараса Шевченка. Військовий інститут. – Київ, 2010. – Вип. 27. – С. 53-56.
6. Дорф Р. Современные системы управления / Р. Дорф, Р. Бишоп; пер. с англ. Б.И. Копылова. – М.: Лаборатория базовых знаний, 2004. – 832 с.

УСТРОЙСТВО РЕГУЛИРОВАНИЯ ПЕРЕМЕННОГО НАПРЯЖЕНИЯ С ПЕРЕСТРАИВАЕМОЙ СИСТЕМОЙ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ

Ю.А. Гунченко[1], А.В. Селюков[2], К.Ф. Боряк[3]

[1] Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: 7996445@mail.ru
[2] ГП «Научный центр точного машиностроения»,
ул. Бориспольская, 9, Киев, 02099, Украина
[3] Одесская государственная академия технического регулирования и качества,
ул. Ковальская, 15, Одесса, 65020, Украина

Проанализированы типы и принципы построения современных регуляторов переменного напряжения – стабилизаторов. Предложена система автоматического управления (САУ) для рассматриваемых устройств с перестраиваемой в зависимости от ошибки регулирования структурой. Приведены диаграммы работы для системы импульсно-фазовой модуляции. Получены передаточные функции САУ, которые справедливы для различных способов регулирования. Предложенная система позволила улучшить основные показатели качества регуляторов напряжения – время установления, перерегулирование, установившаяся ошибка.

Ключевые слова: переменное напряжение, стабилизатор, система импульсно-фазового регулирования (СИФУ), система автоматического управления (САУ), передаточная функция

CONTROL DEVICE AC VOLTAGE WITH VARIABLE AUTOMATIC CONTROL SYSTEM

Yuriy A. Gunchenko[1], Oleksandr V. Selyukov[2], Kostyantyn F. Boryak[3]

[1] Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: 7996445@mail.ru
[2] Scientific center of precision engineering, State enterprise,
9 Boryspilska str., Kyiv, 02099, Ukraine
[3] Odessa State Academy of Technical Regulation and Quality,
15 Kovalska str., Odessa, 65020, Ukraine

There were the types and principles of modern variable voltage regulators – stabilizers analyzed. Automatic control system (ACS) was proposed for the considered devices with tunable depending on the error control structure. Diagrams of the system for pulse-phase modulation were shown. The transfer functions of ACS were obtained, which are valid for different ways of regulation. The proposed system has improved the quality of key performance indicators for voltage regulators – the settling time, overshoot, steady-state error.

Keywords: AC voltage stabilizer, a system of pulse-phase control, an automatic control system, the transfer function

УДК 004: 519.2:519.6

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 1, pp. 64-69

МОДЕЛЮВАННЯ ГАУСІВСЬКИХ ВИПАДКОВИХ ВЕЛИЧИН НА ОСНОВІ ПЕРЕТВОРЕННЯ ДЖОНСОНА ІЗ СІМ'Ї S_B

С.Б. Приходько

Національний університет кораблебудування імені адмірала Макарова,
просп. Героїв Сталінграду, 9, Миколаїв, 54025, Україна; e-mail: sergiy.prykhodko@nuos.edu.ua

Робота присвячена створенню метода моделювання гаусівських випадкових величин на основі нормалізуючого перетворення Джонсона із сім'ї S_B, який, на відміну від існуючих методів, для генерування одного значення гаусівської випадкової величини потребує тільки одне значення випадкової величини з рівномірним розподілом.

Ключові слова: моделювання, випадкова величина, розподіл Гауса, перетворення Джонсона

Вступ

Для моделювання різноманітних випадкових процесів та подій дуже часто виникає потреба в значеннях випадкової величини з розподілом Гауса. Зараз для моделювання гаусівських випадкових величин існує багато методів, які базуються на перетворенні випадкових чисел з рівномірним розподілом у такі, що мають розподіл Гауса [1-3]. Частка з цих методів базується на центральній граничній теоремі і потребує для генерації одного значення гаусівської випадкової величини від 12 значень випадкових чисел з рівномірним розподілом. Інші – використовують спеціальні перетворення (наприклад, Бокса-Мюллера) і потребують на створення певної кількості значень гаусівської випадкової величини приблизно в 1.25 рази більше значень випадкових чисел з рівномірним розподілом. Все це приводе до проблеми додаткових витрат ресурсів комп'ютера на моделювання. Крім того виникає проблема зменшення фактичної кількості значень псевдовипадкових чисел з рівномірним розподілом в межах періоду генератора, яку можна використовувати до їх повторення. Тому ціль даної роботи полягає у побудові метода моделювання гаусівських випадкових величин, який би дозволяв би зменшити витрати ресурсів комп'ютера на відповідне моделювання та максимально використовувати наявні можливості генераторів псевдо-випадкових чисел за рахунок того, що для створення одного значення гаусівської випадкової величини буде потрібно тільки одне значення випадкової величини з рівномірним розподілом. Для цього в роботі пропонується застосувати нормалізуюче перетворення Джонсона із сім'ї S_B.

Метод на основі перетворення Джонсона із сім'ї S_B

В загальному випадку перетворення Джонсона має вигляд [4]

$$z = \gamma + \eta h(x, \varphi, \lambda); \quad \eta > 0; \quad -\infty < \gamma < \infty; \quad \lambda > 0; \quad -\infty < \varphi < \infty, \tag{1}$$

де

z – нормально розподілена випадкова величина з математичним сподіванням нуль і дисперсією одиниця;

x – випадкова величина з розподілом Джонсона;

γ, η, λ, φ – параметри перетворення або розподілу Джонсона;

h – функція з певної сім'ї:

$$h=\begin{cases}\ln(\tilde{x}), & x>\varphi, & \text{для сім'ї } S_L;\\ \ln[\tilde{x}/(1-\tilde{x})], & \varphi<x<\varphi+\lambda, & \text{для сім'ї } S_B;\\ \operatorname{Arsh}(\tilde{x}), & -\infty\le x\le+\infty, & \text{для сім'ї } S_U.\end{cases}$$

Тут $\tilde{x}=(x-\varphi)/\lambda$; $\operatorname{Arsh}(\tilde{x})=\ln\left(\tilde{x}+\sqrt{\tilde{x}^2+1}\right)$.

Для перетворення (1) функції щільності ймовірності (ФЩЙ) випадкової величини x відповідних сімей S_L, S_B, S_U задаються як

$$f_L(x)=\frac{\eta}{\sqrt{2\pi}(x-\varphi)}\exp\left\{-\frac{\eta^2}{2}\left[\frac{\gamma-\eta\ln\lambda}{\eta}+\ln(x-\varphi)\right]^2\right\};$$

$$f_B(x)=\frac{\eta\lambda}{\sqrt{2\pi}(x-\varphi)(\lambda+\varphi-x)}\exp\left\{-\frac{1}{2}\left[\gamma+\eta\ln\left(\frac{x-\varphi}{\lambda+\varphi-x}\right)\right]^2\right\};$$

$$f_U(x)=\frac{\eta}{\sqrt{2\pi\left\{(x-\varphi)^2+\lambda^2\right\}}}\exp\left\{-\frac{1}{2}\left[\gamma+\eta\ln\left(\tilde{x}+\sqrt{\tilde{x}^2+1}\right)\right]^2\right\}.$$

Сім'ї розподілів Джонсона у площині асиметрії у квадраті A^2 та ексцесу ε займають значні області (рис. 1).

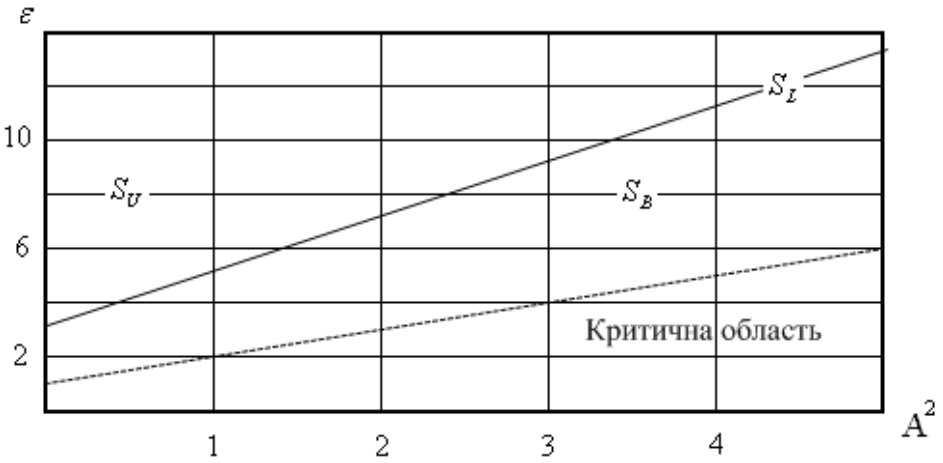

Рис. 1. Комбінації A^2 і ε для розподілів Джонсона

Якщо комбінація A^2 і ε знаходиться біля лінії S_L, то розподіл апроксимується ФЩЙ сім'ї S_L. Розподіл зі значеннями A^2 і ε, які лежать вище лінії S_L, апроксимуються ФЩЙ сім'ї S_U, а які лежать нижче лінії S_L (до лінії критичної

області) – ФЩЙ сім'ї S_B. Якщо комбінація A^2 і ε попадає в критичну область, то вибірковий розподіл не можна апроксимувати розподілом Джонсона.

Параметри для обраної сім'ї розподілів Джонсона можна знайти шляхом рішення наступної задачі математичного програмування [5]:

$$\boldsymbol{\theta} = \arg\min_{\boldsymbol{\theta}} \left\{ \sum_{j=1}^{m} \left[y(x_j) - f(x_j, \theta) \right]^2 \right\}, \tag{2}$$

де

$\boldsymbol{\theta}$ – вектор невідомих параметрів, $\boldsymbol{\theta} = \{\gamma, \eta, \lambda, \varphi\}$;

x_j – значення x в середині j-го підінтервалу;

$y(x_j)$ – значення ординати гістограми для x_j;

$f(x_j, \theta)$ – вираз ФЩЙ для x_j;

m – кількість підінтервалів гістограми.

Оцінювання параметрів розподілу Джонсона за рішенням задачі (2) можна здійснити у разі великої вибірки, коли можна побудувати гістограму. У разі як малої, так і великої вибірок відповідні параметри можуть бути визначені за рішенням задачі [5]

$$\boldsymbol{\theta} = \arg\min_{\boldsymbol{\theta}} \left\{ A_z^2 + (\varepsilon_z - 3)^2 \right\}, \tag{3}$$

де

$$A_z = \frac{1}{nS_z^3} \sum_{i=1}^{n} (z_i - \bar{z})^3;$$

$$\varepsilon_z = \frac{1}{nS_z^4} \sum_{i=1}^{n} (z_i - \bar{z})^4;$$

$$\bar{z} = \frac{1}{n} \sum_{i=1}^{n} z_i;$$

$$S_z^2 = \frac{1}{n} \sum_{i=1}^{n} (z_i - \bar{z})^2;$$

z_i – i-значення величини z у вибірці довжиною n, $i \in [1, n]$, визначаються за (1) або іншим нормалізуючим перетворенням.

Підкреслимо, що в [5] за рішенням задачі (3) здійснювалося оцінювання параметрів різних нормалізуючих перетворень – Джонсона, Бокса-Кокса, Менлі. Для визначення параметрів тільки перетворення Джонсона задачу (3) краще модифікувати наступним чином:

$$\boldsymbol{\theta} = \arg\min_{\boldsymbol{\theta}} \left\{ A_z^2 + (\varepsilon_z - 3)^2 + \bar{z}^2 + (S_z^2 - 1)^2 \right\}. \tag{4}$$

В (4) враховане те, що в перетворенні Джонсона (1) z – це нормально розподілена випадкова величина з нульовим математичним сподіванням і одиничною дисперсією.

Не важко побачити, що для того щоби за перетворенням (1) отримати значення випадкової величини з розподілом Гауса треба мати значення випадкової величини з розподілом Джонсона, яке в свою чергу потрібно отримувати за значенням випадкової величини з рівномірним розподілом. Тоді суть метода моделювання гаусівських випад-

кових величин на основі перетворення Джонсона полягає у наступному. Спочатку генеруємо значення випадкової величини з рівномірним розподілом, яке перетворюємо у значення випадкової величини з розподілом Джонсона певної сім'ї, а потім за допомогою (1) отримуємо значення випадкової величини з розподілом Гауса.

Для практичної реалізації метода, що пропонується, потрібно мати функцію, за допомогою якої значення випадкової величини з рівномірним розподілом можна перетворити у значення випадкової величини з розподілом Джонсона певної сім'ї. У цьому полягає основна складність. У якості такої функції пропонується використати функцію синуса, яка дозволяє отримати значення випадкової величини x з розподілом Джонсона із сім'ї S_B за значення випадкової величини U з рівномірним розподілом за таким перетворенням

$$x = \sin\frac{\pi U}{2},\ U \in [-1, 1]. \tag{5}$$

За (5) отримують вибірку значень випадкової величини x з практично нульовою асиметрією та ексцесом, якій дорівнює 1.5. Ці значення асиметрії та ексцесу і відповідають розподілу Джонсона із сім'ї S_B (рис. 1). Параметри розподілу або перетворення Джонсона із сім'ї S_B визначаємо за рішенням задачі (4). Ці параметри є такими: $\gamma = 2.778474\times10^{-5}$, $\eta = 0.3522056$, $\lambda = 2.0034832$, $\varphi = -1.0017416$.

Тоді значення гаусівської випадкової величини з математичним сподіванням нуль і дисперсією одиниця визначаємо за перетворенням Джонсона (1) із сім'ї S_B із зазначеними вище параметрами (окрім γ) за формулою

$$z = 0.3522056\ln[\tilde{x}/(1-\tilde{x})], \tag{6}$$

де $\tilde{x} = \left(\sin\frac{\pi U}{2} + 1.0017416\right) \Big/ 2.0034832$.

Моделювання значень випадкової величини з розподілом Гауса із використанням нормалізуючого перетворення Джонсона із сім'ї S_B за формулою (6) показало працездатність запропонованого методу. Так, при моделюванні 2000 значень гаусівської випадкової величини z отримано такі її характеристики: ексцес $\varepsilon_z = 2.99998$; асиметрія $A_z = -0.003923$; вибіркове середнє $\bar{z} = -1.269\times10^{-3}$; вибіркова дисперсія $S_z^2 = 0.999997$. Побудована за результатами моделювання гістограма величини z наведена на рис. 2. На рис. 2 пунктиром також показана ФЩЙ розподілу Гауса f_z.

Перевірка гіпотези про нормальність закону розподілу за критерієм Пірсона показала, що з ймовірністю 0.995 змодельовані значення випадкової величини z на інтервалі $m_z \pm 2\sigma_z$ відповідають закону Гауса. Тут m_z – це математичне сподівання величини z, а σ_z – її середнє квадратичне відхилення.

Висновки

Отримав подальший розвиток метод моделювання гаусівських випадкових величин на основі нормалізуючих перетворень за рахунок застосування перетворення Джонсона із сім'ї S_B, який, на відміну від існуючих методів, для створення одного значення гаусівської випадкової величини потребує тільки одне значення випадкової величини з рівномірним розподілом.

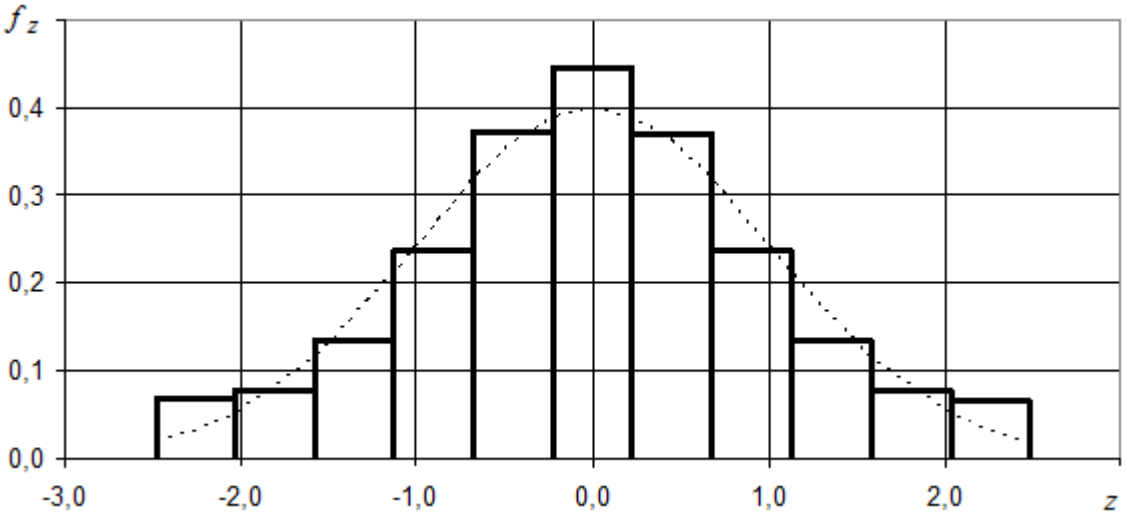

Рис. 2. Емпіричний та теоретичний розподіли випадкової величини z

Вперше отримано перетворення значення випадкової величини з рівномірним розподілом у значення гаусівської випадкової величини з нульовим математичним сподіванням і одиничною дисперсією за рахунок застосування перетворення Джонсона із сім'ї S_B та функції, яка визначає за значеннями випадкової величини з рівномірним розподілом значення випадкової величини з розподілом Джонсона із сім'ї S_B. Отримане перетворення, на відміну від існуючих, для визначення одного значення гаусівської випадкової величини потребує тільки одне значення випадкової величини з рівномірним розподілом. Воно базується на обчисленні двох трансцендентних функцій.

В подальшому планується для моделювання гаусівських випадкових величин застосувати інші сім'ї перетворення Джонсона.

Список літератури

1. Форсайт Дж. Машинные методы математических вычислений [Текст] / Дж. Форсайт, М. Малькольм, К. Моулер ; пер. с англ. Х.Д. Икрамова. – М. : Мир, 1980. – 279 с.
2. Вероятностные методы в вычислительной технике : Учебное пособие для вузов / А.В. Крайников, Б.А. Кудриков, А.Н. Лебедев; Ред. А.Н. Лебедев, Ред. Е.А. Чернявский. – М. : Высшая школа, 1986. – 312 с.
3. Ситник В.Ф. Імітаційне моделювання : Навч. посібник / В.Ф. Ситник, Н.С. Орленко ; Київський національний економічний ун-т. – К. : [б.в.], 1998. – 232 с.
4. Кендалл М. Теория распределений : Пер. с англ. / М. Кендалл, А. Стьюарт ; пер. В.В. Сазонов, пер. А.Н. Ширяев, ред. пер. А.Н. Колмогоров. – М. : Наука, 1966. – 588 с.
5. Приходько С.Б. Інтервальне оцінювання статистичних моментів негаусівських випадкових величин на основі нормалізуючих перетворень / С.Б. Приходько // Математичне моделювання. – Дніпродзержинськ: ДДТУ, 2011. – № 1 (24). – С. 9-13.

МОДЕЛИРОВАНИЕ ГАУССОВСКИХ СЛУЧАЙНЫХ ВЕЛИЧИН НА ОСНОВЕ ПРЕОБРАЗОВАНИЯ ДЖОНСОНА ИЗ СЕМЕЙСТВА S_B

С.Б. Приходько

Национальный университет кораблестроения имени адмирала Макарова,
просп. Героев Сталинграда, 9, Николаев, 54025, Украина; e-mail: sergiy.prykhodko@nuos.edu.ua

Робота посвящена созданию метода моделирования гауссовских случайных величин на основе нормализирующего преобразования Джонсона из семейства S_B, который, в отличие от существующих методов, для генерирования одного значения гауссовской случайной величины требует только одно значение случайной величины с равномерным распределением.

Ключевые слова: моделирование, случайная величина, распределение Гаусса, преобразование Джонсона

MODELLING OF GAUSSIAN RANDOM VARIABLES BASED ON JOHNSON TRANSFORMATION FROM S_B FAMILY

Sergiy B. Prykhodko

Admiral Makarov National University of Shipbuilding,
9 Geroyiv Stalingrada Ave., Mykolayiv, 54025, Ukraine; e-mail: sergiy.prykhodko@nuos.edu.ua

The article is devoted to creation of method for modelling of Gaussian random variables based on Johnson transformation from S_B family, which, unlike existing methods, to generate a Gaussian random variable value requires only one value of a uniform random variable.

Keywords: modelling, random variable, Gaussian distribution, Johnson transformation

УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 1, pp. 70-76

ЕЩЕ ОДИН ПОДХОД К МОДЕЛИРОВАНИЮ ПРОТИВНИКА ИНФОРМАЦИОННОЙ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ ТЕОРИИ ГРАФОВ

И.И. Борисенко, В.М. Рувинская

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

В работе построена графовая модель противника информационной системы и показано, как удобная укладка графа, полученная благодаря разбиению графа на классы эквивалентности и порядка, может сыграть принципиально важную роль в решении задачи уничтожения или ограничения деятельности криминальной группировки.

Ключевые слова: графовая модель, классы эквивалентности и порядка, информационная система, противник

Введение

В настоящее время в научном мире ведется активная работа по математическому моделированию террористических организаций и других типов криминальных групп. Традиционным путем для представления группы людей с указанием взаимных отношений между ними является использование теории графов. Это обусловлено рядом факторов, среди которых наглядность получаемой модели, возможность адекватного отражения при помощи стандартных операций на графах реальных действий над группами и событий в группах, существованием разработанного математического аппарата для работы с графами, включая большое количество хорошо зарекомендовавших себя на практике эвристических методов обработки [1, 2].

До недавнего времени существовавшие модели террористической группировки не отражали ее реальную иерархию и взаимосвязь между членами в полной мере, что не позволяло удовлетворительно формализовать решение таких задач, как уничтожение или ограничение деятельности криминальной организации. Лишенная указанных недостатков модель была предложена в [3]. Авторами была разработана общая графовая модель произвольной группы противника со строго обоснованным учетом иерархии этой группы при помощи взвешенного неориентированного графа. Отдельные индивидуумы представляются в такой модели в виде узлов (вершин), пары которых соединяются ребром при существовании определенной взаимосвязи между соответствующими членами рассматриваемой группы. Введение значений веса для вершин и ребер происходит при максимальном использовании априорной информации о моделируемом противнике и имеет определяющее значение в предлагаемой модели. Среди основных факторов, которые влияют на формирование веса вершины, выделяются: осведомленность члена группы о возможностях средств защиты информации, используемых в системе и представляющих интерес для данного индивидуума; материальные и временные возможности противника; роль рассматриваемого члена в группе противника. Кроме того, следует учитывать, знает ли потенциальный нарушитель функциональные особенности системы, обладает ли высоким уровнем знаний в области программирования и проектирования, опытом работы с техническими средствами, вычислительной

техникой и так далее. Вес ребра учитывает реальную ценность информации, передаваемой по линии связи, которой оно соответствует, надежность рассматриваемой линии связи. Как видим определение весовых значений не является тривиальной задачей даже при наличии всей необходимой информации и еще более усложняется в случае, если такую информацию надо собрать.

Целью данной работы является разработка такой графовой модели противника, которая позволила бы при ее создании отказаться от использования взвешенного графа, что привело бы к упрощению ее построения и анализа.

Для достижения цели следует решить *задачи*: построить ориентированный граф, отражающий информационные связи некоторой группировки; представить исходный граф в максимально простом и удобном виде для его анализа благодаря алгоритмам разбивки графа на классы эквивалентности и порядка; разработать такие алгоритмы.

Орграф противника и его морфологический анализ

Будем рассматривать противника информационной системы (ИС) как частный случай террористической группы, а его математическую модель представим ориентированным графом. Отдельные индивидуумы представляются в такой модели в виде узлов (вершин), пары которых соединяются ориентированным ребром при существовании определенной направленной взаимосвязи между ними (такой, например, как передача информации в определенном направлении или иерархия между соответствующими членами рассматриваемой группы), исходя из априорной информации о моделируемом противнике. Пример графовой модели противника представлен на рис. 1. Реальные модели могут иметь достаточно сложную структуру, в которых предугадать иерархию вершин невозможно, поэтому перейдем к более удобной его укладке.

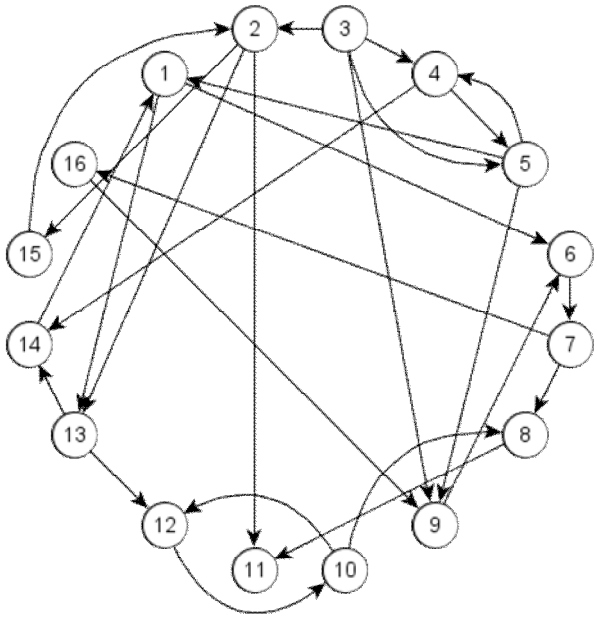

Рис. 1. Пример графовой модели противника

Одной из основных задач, которые решаются по морфологическому анализу ориентированных графов, является разбиение множества его вершин на классы эквивалентности и порядка.

Под классом эквивалентности ориентированного графа подразумевается его сильно связанный подграф, где смысл сильной связи заключается в достижимости любой вершины из любой вершины данного класса [4]. Для всякой вершины i орграфа можно определить прямое $G^{+}(i)$ и обратное $G^{-}(i)$ транзитивные замыкания. Смысл прямого транзитивного замыкания $G^{+}(i)$ состоит в том, что оно указывает множество вершин орграфа в которые можно попасть из вершины i. Обратное транзитивное замыкание $G^{-}(i)$ указывает на те вершины, из которых можно попасть в вершину i. Пересечение прямого и обратного транзитивных замыканий определяет подграф сильно связанных вершин или класс эквивалентности вершины i: $C(i) = G^{+}(i) \cap G^{-}(i)$. Например, для графа, представленного на рис. 1 и $i = 1$ имеем:

$$G^{+}(1) = \{1,6,7,8,9,10,11,12,13,14,16\};$$

$$G^{-}(1) = \{1,2,3,4,5,13,14,15\}.$$

Следовательно, первый класс сильно связанных вершин образован вершинами:

$$C_1(1) = G^{+}(1) \cap G^{-}(1) = \{1,13,14\}.$$

Для $i = 2$: $G^{+}(2) = \{2,11,15\}$; $G^{-}(2) = \{2,3,15\}$; $C_2(2) = \{2, 15\}$. Аналогично определяются оставшиеся классы эквивалентности: $C_3 = \{3\}$; $C_4 = \{4, 5\}$; $C_5 = \{6,7,9, 16\}$; $C_6 = \{12, 10\}$; $C_7 = \{8\}$; $C_8 = \{11\}$.

Используя полученные классы эквивалентности, выполним другую укладку исходного графа, так, как показано на рис. 2, из которой видно, что сильно связанные подграфы подчинены отношению порядка. Такой граф легко поддается анализу.

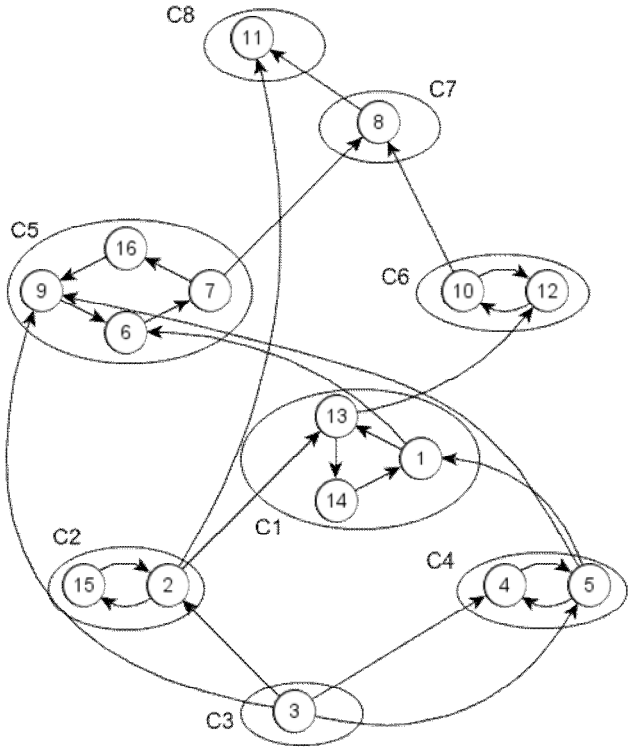

Рис. 2. Графовая модель противника с выделенными сильно связанными подграфами

Построение классов эквивалентности и порядка

Чтобы алгоритмизировать процесс нахождения классов эквивалентности, воспользуемся матрицей смежности графа, которая однозначно задает его структуру [5]. Массив матрицы смежности (назовем его Adj) для рассматриваемого графа имеет вид:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0
2	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0
3	0	1	0	1	1	0	0	0	1	0	0	0	0	0	0	0
4	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0
5	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0
6	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
8	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
9	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0
14	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0

Для хранения информации о прямом и обратном транзитивном замыкании некоторой вершины создаются дополнительные массивы $G\_plus(n)$ и $G\_negativ(n)$, где $n=16$ – количество вершин графа. Опишем последовательность действий заполнения этих массивов для $i=1$. В массивы $G\_plus(1)$ и $G\_negativ(1)$ записываем 0.

Поскольку транзитивные замыкания будут строиться для вершины с номером 1, то в первой строке массива Adj ищем единицы – они находятся в шестом и тринадцатом столбце, это означает, что наименьшее расстояние, равное одной дуге, от вершины с номером 1 до вершин с номерами 6 и 13. Поэтому в массив $G\_plus(6)$ и $G\_plus(13)$ записываем по 1. Далее в шестой строке массива Adj находим единицу в столбце 7 и в тринадцатой строке по единице в столбце 12 и 14. Это означает, что по две дуги отделяет вершину с номером 1 от вершин с номерами 7, 12 и 14, поэтому в *G_plus*(7), *G_plus*(12) и *G_plus*(14) записываем число 2 и так далее. Ячейка *G_plus* заполняется лишь в том случае, если она пуста (при построении соответствующего алгоритма здесь и далее ячейка считается пустой, если, например, её значение отрицательно). Аналогичным образом заполняется массив G*_negativ*, но в этом случае используются не строки, а столбцы массива Adj. В результате получим:

G_plus:

0					1	2	3	4	3	4	2	1	2		3
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

G_negativ:

0	3	2	2	1								2	1	4	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Далее анализируем полученные массивы: если ячейка с одним и тем же индексом не пуста и в *G_plus* и в *G_negativ*, то вершина ей соответствующая будет принадлежать

искомому классу эквивалентности. В нашем случае это ячейки с номерами 1, 13, 14. Сохраняем этот список, а вершины 1, 13, 14 из массива Adj удаляем, таким образом переходим к некоторому массиву Adj^* из которого выбираем произвольную вершину для построения следующего класса эквивалентности.

Как указывалось выше, граф, представленный на рис. 2, достаточно легко поддается анализу, поскольку упорядочение его классов эквивалентности вполне очевидно. В реальных условиях это бывает не так. Поэтому рассмотрим простой алгоритм разложения орграфа на классы порядка. Разбиению на классы порядка поддаются только орграфы, которые не содержат контуров и петель, если же таковые имеются, то первоначально следует выполнить разбивку множества вершин на классы эквивалентности, а затем каждый из классов принять за вершину нового орграфа. В нашем случае новый орграф будет иметь восемь вершин $C1,\ldots,C8$. Составим его матрицу смежности и запишем ее в массив Adj_factor. Adj_factor имеет вид:

	1	2	3	4	5	6	7	8
1	0	0	0	0	1	1	0	0
2	1	0	0	0	0	0	0	1
3	0	1	0	1	1	0	0	0
4	1	0	0	0	1	0	0	0
5	0	0	0	0	0	0	1	0
6	0	0	0	0	0	0	1	0
7	0	0	0	0	0	0	0	1
8	0	0	0	0	0	0	0	0

На каждом шаге алгоритма надо выявить столбцы, в которых отсутствуют единицы, такой столбец на первом шаге алгоритма имеет номер 3 и соответствует вершине $C3$, которая представляет самый нижний уровень в иерархии классов порядка, обозначим этот класс $P1$; вершине $C3$ не предшествует ни одна дуга и она является «истоком». Удаляем третью строку и третий столбец, которые соответствуют вершине $C3$, переходим к массиву Adj_factor^*. Снова отыскиваем столбцы, в которых отсутствуют единицы – это столбцы с номерами 2 и 4, значит вершины $C2$ и $C4$ образуют класс P2 и т.д. В результате получим шесть классов порядка: $P1 - C3$; $P2 - C2$, $C4$; $P3 - C1$; $P4 - C5$, $C6$; $P5 - C7$; $P6 - C8$. Граф с разбивкой на классы порядка представлен на рис. 3.

Следует сделать замечание, что сразу следует начинать разбивку графа на классы порядка, что предотвращает лишнюю работу. Если бы на каком- то шаге не появился столбец, не содержащий единиц, то это означало бы, что исходный граф содержит контуры и требуется предварительная разбивка его на классы эквивалентности. Например, если бы в нашем случае мы сразу начали выделять классы порядка, минуя этап разбивки на классы эквивалентности, то на первом шаге у нас нашёлся бы столбец, в котором не было бы единиц – это столбец под номером 3 (см. массив Adj), но уже на втором шаге мы такого столбца не получим.

Выводы

Традиционно графовые модели противника служат для решения следующих задач [3]:

1) Определение членов противника, блокирование которых приведет к распаду организации на несколько несвязных между собой подгрупп, что приведет как к полно-

му прекращению ее функционирования, так и к снижению эффективности ее деятельности;

2) Выделение в организации противника таких связей между ее членами, удаление которых приводит к распаду группы на отдельные части, несвязанные между собой, что очевидно ограничит информационные возможности криминальной структуры.

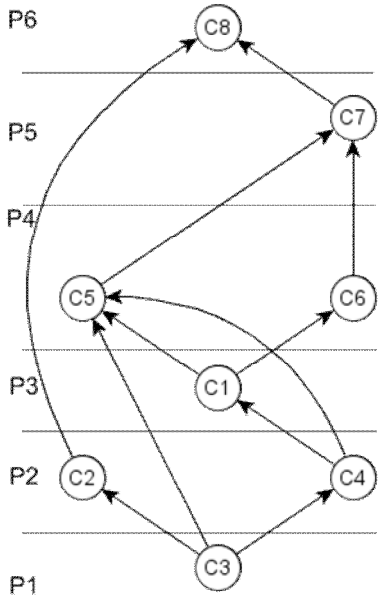

Рис. 3. Графовая модель противника с разбивкой на классы порядка

В теории графов первая задача соответствует задаче определения минимального количества узлов, а вторая – задаче определения минимального количества ребер, удаление которых приведет исходный связный граф к несвязному. Проанализируем модель противника (рис. 3) с точки зрения сказанного. Блокирование подгрупп $C2$ и $C7$, а также разрушение связи $(C1, C6)$ приводит к распаду группы на пять подгрупп. Более того, только одна подгруппа останется связана с «истоком» – этот узел следует трактовать как руководящее звено. С другой стороны, удаление связей $(C2, C8)$ и $(C7, C8)$ приведет также к несвязному графу, но приведет ли это к ощутимым потерям, поскольку блокированы будут только три члена группы? Напротив, блокирование только подгруппы $C5$ приведет к серьезному нарушению информационных потоков и, по-видимому, нанесет ощутимый урон.

Исходя из сказанного можно сделать вывод, что хотя количественную оценку понесенных потерь противника по полученной графовой модели сделать нельзя, это не умаляет ее достоинств, поскольку предложенная модель отражает в полной мере (конечно, исходя из априорной информации, которую в дальнейшем можно уточнять) структуру предполагаемой организации и дает возможность планировать контрмеры по ослаблению ее деятельности. Немаловажным достоинством, является отказ от использования взвешенного графа, что существенно упростило построение модели, а использование ориентированного графа позволило применить простые алгоритмы разбиения его на классы эквивалентности и порядка, что приводит к простому представлению сложных и запутанных исходных графов.

Список литературы

1. Кобозева А.А. Использование взвешенного графа при моделировании террористической сети / А.А. Кобозева, В.А. Хорошко // Інформаційні технології та комп'ютерна інженерія. – 2007. – №3(10). – С. 61-67.
2. Кобозева А.А. Использование теории графов для анализа структуры террористических сетей / А.А. Кобозева, В.А. Хорошко // Захист інформації. – 2008. – №1 – С. 22-31.
3. Кобозева А.А. Анализ информационной безопасности / А.А. Кобозева, В.А. Хорошко. – К. : Изд. ГУИКТ, 2009. – 251 с.
4. Акимов О.Е. Дискретная математика: логика, группы, графы [Текст] / О.Е. Акимов. – 2-е изд., доп. – М. : Лаборатория Базовых Знаний, 2003. – 376 с.
5. Харари Ф. Теория графов / Ф. Харари; пер. с англ. В.П. Козырева. – М. : Мир, 1973. – 300 с.

ЩЕ ОДИН ПІДХІД ДО МОДЕЛЮВАННЯ СУПРОТИВНИКА ІНФОРМАЦІЙНОЇ СИСТЕМИ З ВИКОРИСТАННЯМ ТЕОРІЇ ГРАФІВ

І.І. Борисенко, В.М. Рувінська

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

У роботі побудована графова модель супротивника інформаційної системи і показано, як зручне укладання графа, отримане завдяки розбиттю графа на класи еквівалентності і порядку, може зіграти принципово важливу роль в вирішенні задачі знищення або обмеження діяльності кримінального угрупування.

Ключові слова: графова модель, класи еквівалентності і порядку, інформаційна система, супротивник

ANOTHER APPROACH TO THE MODELING OF OPPONENT OF THE INFORMATION SYSTEM WITH THE USE OF THEORY OF THE GRAPHS

Iryna I. Borysenko, Viktoria M. Ruvinskaya

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

In this work the graph model of opponent of the information system had built and was showed that a comfortable piling of the graph got due to the selection of classes of equivalence and order, that can play an important role in the decision of task of elimination or limitation of activity of criminal groupment.

Keywords: graph model, classes of equivalence and order, information system, opponent

УДК 330.43

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 1, pp. 77-86

РАЗРАБОТКА СЕМАНТИЧЕСКОГО ЯДРА САЙТА С ДИНАМИЧЕСКИМ КОНТЕНТОМ НА ОСНОВЕ АССОЦИАТИВНЫХ ПРАВИЛ

Е.А. Арсирий, О.А. Игнатенко, А.А. Леус

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

В результате анализа проблем продвижения в поисковых системах веб-ресурсов с динамическим контентом предложена методика разработки семантического ядра сайта на основе создания ассоциативных правил с помощью алгоритма поиска популярных наборов Apriori в транзакционной базе данных поисковых запросов. Применение методики позволило повысить полноту и точность, а также снизить время разработки семантического ядра сайта типа Интернет-витрины и магазина.

Ключевые слова: поисковая система, поисковые запросы, семантическое ядро сайта, популярные наборы, ассоциативные правила, алгоритм Apriori

Введение

В век информационных технологий успех практически любого бизнеса в достаточно большой степени зависит от способов виртуального представления фирмы в сети Интернет. При этом целью разработки контента веб-ресурса фирмы является предоставление информации, которая была бы способна заставить пользователя думать и вести себя в направлении, выгодном реальному бизнесу. С другой стороны, известно, что доля «поискового трафика» любого сайта (число посетителей, пришедших от поисковых выдач, от общей посещаемости сайта) является преобладающей [1,2]. Поэтому при разработке контента сайта большое внимание уделяется SEO (*search engine optimization*) – комплексу мер, направленных на продвижение веб-ресурса к верхним позициям поисковой системы (ПС) с целью увеличения его посещаемости. Известно, что одним из ключевых этапов SEO является разработка семантического ядра сайта (СЯС), которая, как правило, выполняется специалистами вручную и требует больших временных затрат [3, 4]. Такое положение является особенно недопустимым при разработке СЯС с динамическим контентом, когда SEO-специалисты не успевают вовремя реагировать на изменяющиеся наполнение сайта, внешнее Интернет-окружение, а также предпочтения и действия пользователей. Поэтому актуальным является создание методики разработки СЯС, применение которой SEO-специалистами позволило бы сократить время на достижение и поддержание лидирующих позиций сайта в поисковых выдачах, что является целью настоящей работы. Для разработки методики авторам необходимо было решить ряд задач:

- проанализировать опосредованную связь между этапами и процедурами работы ПС и разработкой СЯС и предложить метод ее описания;
- определить требования к формированию транзакционной базы данных в терминах анализа связей и разработать базу данных для поисковых транзакций;
- разработать методику применения анализа связей в транзакционной базе поисковых запросов;

- предложить методику реализации поиска популярных наборов с помощью алгоритма *Apriori* и разработки АП на основе найденных популярных наборов для разработки СЯС.

Анализ этапов и процедур работы поисковых систем и разработки семантического ядра сайта

ПС представляет собой сайт, состоящий из веб-интерфейса для пользователя и поисковой машины, которая является движком, обеспечивающим функциональность ПС. Поисковая машина состоит из модуля индексирования, базы данных (БД) проиндексированных документов и поискового сервера, занимающегося анализом и обработкой запросов пользователей. Модуль индексирования состоит из трех вспомогательных программ (роботов) – *spider* (паук), *crawler* (путешествующий паук) и *indexer* (индексатор). *Spider* скачивает веб-документы с помощью протокола HTTP, извлекает ссылки и перенаправления и сохраняет текст в следующем формате: URL, дата скачивания, http-заголовок ответа сервера, тело страницы (html-код). *Crawler* обрабатывает найденные пауком ссылки и осуществляет дальнейшее направление паука. *Indexer* разбирает html-код страницы на составные части такие как заголовки (*title*), подзаголовки (*subtitles*), метатэги (*meta tags*), текст, ссылки, структурные и стилевые особенности и т.д., анализирует их на основе различных лексических и морфологических алгоритмов с целью последующего ранжирования по степени важности. При этом найденным словам и словосочетаниям присваиваются весовые коэффициенты в зависимости от того, сколько раз и где они встречаются (в заголовке страницы, в начале или в конце страницы, в ссылке, в метатэге и т.п.). В результате формируется файл, содержащий индекс, который может быть довольно большим. Для уменьшения его размеров прибегают к минимизации объема информации и сжатию файла, а также решают задачи определения дубликатов и «почти дубликатов». Результаты индексирования записываются в базу данных (БД) проиндексированных документов (рис. 1, а).

Поисковый сервер является важнейшим элементом всей ПС, так как от алгоритмов, которые лежат в основе его функционирования, зависит качество и скорость поиска. Принцип его работы заключается в следующем. Полученный от пользователя запрос (ключевые слова) подвергается морфологическому анализу для получения информационного окружения. При этом выделяются информационные (поиск сведений), транзакционные (совершение действия), нечеткие (общие) и навигационные (прямой адрес) запросы. Поиск документов по их содержанию называется семантическими. Информационное окружение передается специальному модулю ранжирования, задача которого состоит в поиске html-страниц в БД проиндексированных документов, сортировке и выдаче в порядке релевантности. При этом для оценки релевантности найденных документов, как правило, используют *TF-IDF*-меру, согласно которой релевантность документа будет выше, если слово или словосочетание из запроса *чаще* встречается в найденном документе (TF) и *реже* в других документах БД (IDF). Если необходимо, порядок выдачи документов может быть изменен пользователем путем задания дополнительных условий (расширенный поиск). Далее генерируется сниппет, то есть, для каждого найденного документа из таблицы документов извлекаются заголовок, краткая аннотация, наиболее соответствующая запросу и ссылка на сам документ, причем найденные слова подсвечиваются. Полученные результаты поиска передаются пользователю в виде *SERP* (*Search Engine Result Page*) – страницы выдачи поисковых результатов. Таким образом, основой работы всех ПС является определение так называемых «ключевых слов» веб-ресурса. Из списка таких слов состоит семантическое ядро сайта (СЯС). СЯС представляет собой список ключевых слов и их комбинаций, записанных в метатэги *keywords* и распределенных в контенте сайта, а именно, в тэге *title*, в alt-аттрибутах, в ссылочном тексте внутренних и внешних ссылок, в

выделениях жирным и наклонным шрифтом, в начале контента сайта, в названии файлов, в URL и др. При этом от полноты и точности разработки СЯС зависит положение сайта в списке выдач ПС.

Разработка СЯС является ключевым этапом SEO и состоит из ряда интеллектуальных, трудноформализуемых этапов и процедур, для реализации которых необходимы большие временные и человеческие ресурсы (рис. 1, б).

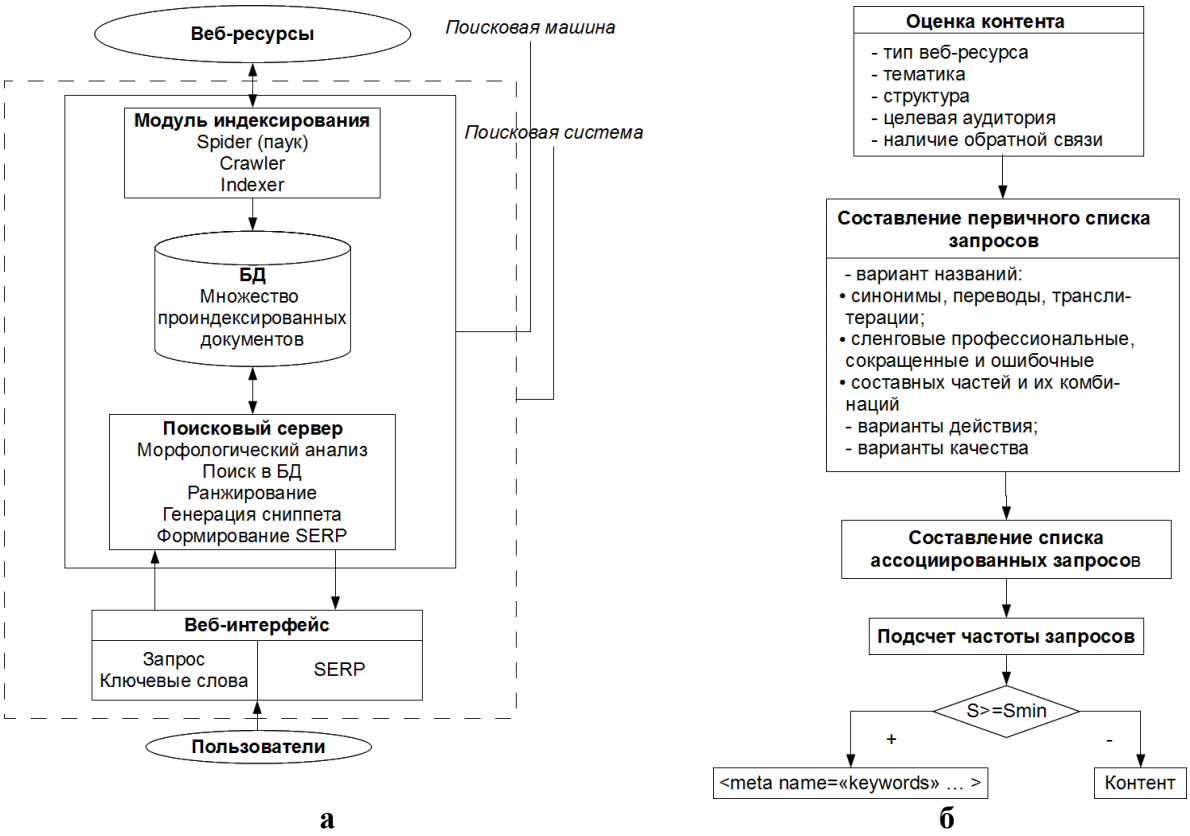

Рис. 1. Обобщенная схема этапов и процедур: а – работы ПС; б – разработки СЯС

На первом этапе необходимо оценить контент сайта, определив его тип (магазин, новостной блог, сайт-визитка и пр.), тематику, структуру, целевую аудиторию и необходимость обратной связи с пользователями. Следующим этапом будет создание первичного списка запросов. Для этого можно использовать различные варианты названий товаров, услуг, самого сайта, различные действия, предоставляемые пользователям и варианты качества товара или услуг [1]. Затем составляется список ассоциированных запросов с помощью средств статистики поисковых систем (wordstat.yandex, adstat.rambler, adwords.google и др.) и подсчитывается частота ключевых слов. Ключевые слова с наибольшей частотой помещают в метатэги *keywords*, с меньшей – распределяют по контенту сайта. Однако, для сайтов с динамическим контентом, таких как Интернет-витрина и магазин, новостной блог, где меняется ассортимент товаров, их популярность, новости, заголовки и пр., перечисленные этапы разработки СЯС необходимо повторять достаточно часто. При этом длительность выполнения каждого этапа может значительно задерживать необходимую периодичность повторения, что приводит к снижению полноты и точности СЯС, а сайт теряет свои позиции в SERP. Для сокращения времени разработки СЯС с динамическим контентом без потери полноты и точности в данном исследовании предлагается использовать анализ связей (*link analysis*), позволяющий сгенерировать правила количественного описания взаимной связи между двумя и более ключевыми словами, объединенными в одном семанти-

ческом запросе. Такие правила в терминах анализа связей называются *ассоциативными*, а запрос представляет собой некоторое множество событий происходящих совместно и образует *транзакцию*.

Транзакционная или операционная БД представляет собой двумерную таблицу, которая состоит из номера транзакции (TID) и перечня ключевых слов, составивших запрос во время этой транзакции. Пример фрагмента транзакционной БД (ТБД) для Интернет-витрины Konica-Digital показан в табл. 1, где TID – уникальный идентификатор, определяющий каждый поисковый запрос или транзакцию. На основе имеющейся транзакционной базы данных необходимо найти закономерности между событиями, то есть запросами пользователей.

Таблица 1.

Транзакционная база данных (фрагмент)

TID	Поисковые запросы			
1	флешки	онлайн		
2	*фото*	*альбом*		
3	*фото*	*альбом*	онлайн	
4	фото	рамки		
5	фото	рамки	купить	онлайн
6	печать	фото	онлайн	
7	фото	магазин		
8	фото	рамки	онлайн	
9	печать	фото		
10	интернет	магазин	фото	
11	*фото*	магазин	*альбом*	
12	фото	магазин	рамки	
13	рамки	*альбом*	*фото*	
14	печать	флешки		

Пусть $I = \{i_1, i_2, i_3, \ldots, i_n\}$ – множество (набор) ключевых слов, называемых элементами. Пусть D – множество транзакций из ТБД, где каждая транзакция T с уникальным номером TID – это набор элементов из I, $T \subseteq I$. Каждая транзакция представляет собой бинарный вектор, где $t[k] = 1$, если i_k элемент присутствует в транзакции, иначе $t[k] = 0$. При этом транзакция T содержит A, некоторый набор элементов из I, если $A \subseteq T$ (табл. 2). Ассоциативным правилом (АП) состоящим из двух наборов элементов называется импликация $A \to B$, где $A \subset I$, $B \subset I$ и $A \cap B = \varnothing$. При этом A называют условием (*antecedent*), а B – следствием (*consequent*) и говорят «если A, то B». Можно выделить объективные (независимые от конкретного приложения) и субъективные (связанные с контекстом задачи) меры значимости АП. К объективным мерам, описывающим связь между наборами элементов, которые соответствуют условию и следствию, относят поддержку – *supp* (*support*) и достоверность *conf* – (*confidence*).

Правило $A \to B$ имеет поддержку *supp*, если *supp%* транзакций из D, содержат $A \cup B$ (условие и следствие), т.е.

$$supp(A \to B) = supp(A \cup B). \quad (1)$$

Достоверность *conf* правила – отношение количества транзакций, содержащих условие A и следствие B, к количеству транзакций, содержащих только условие A – показывает какова вероятность того, что из A следует B

$$conf(A \to B) = supp(A \cup B)/supp(A). \quad (2)$$

При этом говорят, правило $A \to B$ справедливо с достоверностью *conf*, если *conf%* транзакций из D, содержащих A, также содержат B.

Целью анализа связей является получить возможные АП вида $A \to B$ для всех элементов с различными значениями поддержки и достоверности, которые должны быть выше определенных порогов, называемых соответственно минимальной поддержкой (*minsupport*) и минимальной достоверностью (*minconfidence*). При этом следует учитывать случаи, когда условие и следствие являются независимыми ($\text{supp}(A \to B) \approx \text{supp}(A) \cdot \text{supp}(B)$) не смотря на высокие значения поддержки и достоверности. Такое АП не является значимым. Поэтому для оценки значимости правила используют также субъективные меры, которым относят *lift* («интерес») и *leverage* («плечо»).

Lift – отношение частоты появления условия в транзакциях, которые содержат также и следствие, к частоте появления следствия в целом

$$lift(A \to B) = conf(A \to B)/supp(B) = (supp(A \cup B)/supp(A))/supp(B),$$
$$lift(A \to B) = supp(A \cup B)/supp(B) \cdot supp(A). \quad (3)$$

Таблица 2.

Транзакционная база данных 1-элементных наборов в нормализованном виде

Элементы	i_1	i_2	i_3	i_4	i_5	i_6	i_7	i_8	i_9
Значения	флешки	онлайн	фото	альбом	рамки	купить	печать	магазин	интернет
1	1	1	0	0	0	0	0	0	0
2	0	0	1	1	0	0	0	0	0
3	0	1	1	1	0	0	0	0	0
4	0	0	1	0	1	0	0	0	0
5	0	1	1	0	1	1	0	0	0
6	0	1	1	0	0	0	1	0	0
7	0	0	1	0	0	0	0	1	0
8	0	1	1	0	1	0	0	0	0
9	0	0	1	0	0	0	1	0	0
10	0	0	1	0	0	0	0	1	1
11	0	0	1	1	0	0	0	1	0
12	0	0	1	0	1	0	0	1	0
13	0	0	1	1	1	0	0	0	0
14	1	0	0	0	0	0	1	0	0
supp (i_k)	14.3	35.7	85.7	28.6	35.7	7.14	21.43	28.6	7.14
minsupp 28.6%		*itemset*$_1$	*itemset*$_1$	*itemset*$_1$	*itemset*$_1$			*itemset*$_1$	

«Лифт» является обобщенной мерой связи двух наборов элементов. Если $lift(A \to B) > 1$, то связь является положительной, если $lift(A \to B) = 1$ – наборы A и B независимы, если $lift(A \to B) < 1$ – связь является отрицательной.

«Плечо» – разность между наблюдаемой частотой, которой условие и следствие появляются совместно (поддержкой ассоциации) и произведением частот появления условия и следствия в отдельности

$$lever(A \to B) = supp(A \cup B) - supp(A) \cdot supp(B). \quad (4)$$

Реализация анализа связей в ТБД, как правило, включает два этапа:

1) Поиск всех наборов элементов, поддержка которых больше либо равна *minsupp*. Такие наборы элементов называются популярными наборами (*frequent itemset*).

2) Разработка АП на основе популярных наборов с достоверностью большей либо равной *minconf*.

Поиск популярных наборов на основе перебора всех возможных наборов элементов из ТБД потребует $O\left(2^{|I|}\right)$ операций, где $|I|$ – количество элементов, при этом с ростом числа элементов в $I(|I|)$ экспоненциально растет число потенциальных наборов элементов.

Для снижения размерности пространства поиска используют свойство антимонотонности поддержки наборов элементов, заключающееся в том, что поддержка любого набора элементов не может превышать минимальной поддержки любого из его поднаборов. Если все возможные наборы элементов из I можно представить в виде решетки связей, начинающейся с пустого набора, затем на 1 уровне располагаются 1-элементные наборы, на 2-м – 2-элементные и т.д. На k-м уровне представлены k-элементные наборы, связанные со всеми своими (k-*1*)-элементными поднаборами (рис. 2). Предположим, что набор из элементов $\{i_1 i_2\}$ согласно (1) имеет поддержку ниже заданного порога и, соответственно, не является популярным. Тогда, согласно свойству антимонотонности, все его постнаборы также не являются популярными и отбрасываются. На рис. 2 – это часть решетки, начиная с $\{i_1 i_2\}$. Таким образом, любой k-элементный набор будет популярным тогда и только тогда, когда все его (k-*1*)-элементные поднаборы будут популярными.

Разработка АП на основе найденных популярных наборов выполняется после расчета поддержки и достоверности, используя (1) и (2) для всех импликаций типа $A \to B$. При этом в качестве A используются все возможные популярные и непустые (k-*1*)-элементные поднаборы $itemset_{k\text{-}1}$ популярного k-элементного набора $itemset_k$, а в качестве B – разности R между $itemset_k$ и всеми $itemset_{k\text{-}1}$. Например (см. рис. 2), для набора $itemset_3 = \{i_1 i_2 i_4\}$ поднаборами будут $itemset_2 = \{\{i_1 i_3\}, \{i_1 i_4\}, \{i_3 i_4\}\}$, а разностями $R = \{\{i_4\}, \{i_3\}, \{i_1\}\}$ соответственно, тогда все импликации $A \to B$ будут выглядеть, как $A \to B = \{(\{i_1 i_3\} \to \{i_4\}), (\{i_1 i_4\} \to \{i_3\}), (\{i_3 i_4\} \to \{i_1\})\}$. При этом импликация $A \to B$ будет относится к АП тогда и только тогда, когда $supp(A \to B) > minsupp$ и $conf(A \to B) > minconf$.

На этапе поиска популярных наборов можно выделить два процедуры: генерация наборов и расчет поддержки набора. Первые алгоритмы поиска популярных наборов (AIS и SETM) генерировали наборы и рассчитывали поддержку во время чтения транзакций из ТБД, не используя при этом свойство антимонотонности [6].

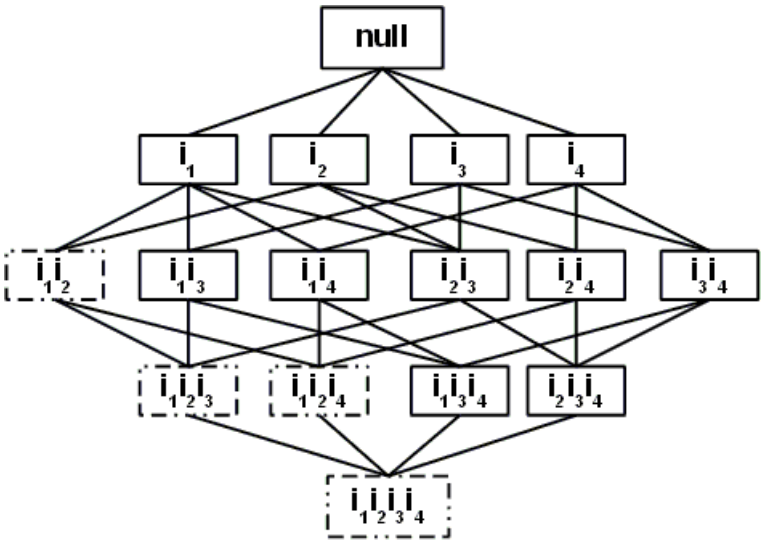

Рис. 2. Решетка связей возможных наборов элементов из ТБД для $I = \{i_1, i_2, i_3, i_4\}$

Сокращение времени поиска популярных наборов можно добиться за счет использования алгоритма *Apriori*. Работа данного алгоритма состоит из некоторого числа (проходов) повторяющихся процедур генерации *k*-элементных наборов-кандидатов (*candidate generation*) и подсчета поддержки наборов-кандидатов (*candidate counting*). При этом генерация кандидатов заключается в создании множества *k*-элементных кандидатов (где *k* – номер этапа) в результате чтения транзакций из ТБД. В отличие от алгоритмов AIS и SETM поддержка при этом не рассчитывается. При подсчете поддержки кандидатов вычисляется поддержка каждого *k*-элементного набора-кандидата и выполняется удаление кандидатов, поддержка которых меньше *minsupp*. Оставшиеся *k*-элементные наборы считаются популярными. В табл. 2, 3 и 4 показаны результаты работы первого, второго и третьего прохода алгоритма *Apriori* с 1-, 2- и 3-элементными наборами-кандидатами.

Количество повторяющихся проходов *k* алгоритма *Apriori*, как правило, равно количеству элементов в самом длинном наборе. В данном примере самым длинным является 4-элементный набор (см. табл. 1) для транзакции с пятым номером: $TID = 5$, $k = 4$. Однако, поддержка ни одного из 3-элементных наборов-кандидатов не больше *minsupp*, поэтому процесс поиска популярных наборов завершается уже после 3-го прохода, и можно переходить ко второму этапу анализа связей в ТБД – разработки АП на основе найденных популярных наборов.

Для разработки АП будут использованы только 2-элементные популярные наборы, т.к. уже отмечалось, что $supp(\bullet)$ ни одного из 3-элементных наборов-кандидатов не больше *minsupp* (см. табл. 4).

На основе 2-элементные популярных наборов сформируем все возможные импликации типа $A \to B$ и рассчитаем их поддержку и достоверность, результаты запишем в табл. 5. Согласно табл. 5, для $minconf = 60\%$ к АП можно отнести следующие правила: «если фото, то онлайн»; «если фото, то альбом»; «если фото, то рамки»; «если фото, то магазин».

Таблица 3.

Транзакционная база данных 2-элементных наборов в нормализованном виде

Элементы	$i_3 i_4$	$i_2 i_4$	$i_2 i_5$	$i_2 i_8$	$i_3 i_4$	$i_3 i_5$	$i_3 i_8$	$i_4 i_5$	$i_4 i_8$	$i_5 i_8$
Значения	онлайн фото	онлайн альбом	онлайн рамки	онлайн магазин	фото альбом	фото рамки	фото магазин	альбом рамки	альбом магазин	рамки магазин
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	1	0	0	0	0	0
3	1	1	0	0	1	0	0	0	0	0
4	0	0	0	0	0	1	0	0	0	0
5	1	0	1	0	0	1	0	0	0	0
6	1	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	1	0	0	0
8	1	0	1	0	0	1	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	1	0	0	0
11	0	0	0	0	1	0	1	0	1	0
12	0	0	0	0	0	1	1	0	0	1
13	0	0	0	0	1	1	0	1	0	0
14	0	0	0	0	0	0	0	0	0	0
supp ($i_k i_j$)	28.6	7.14	14.3	0	28.6	35.7	28.6	7.14	7.14	7.14
minsupp 28.6%	$itemset_2$				$itemset_2$	$itemset_2$	$itemset_2$			

Таблица 4.

Транзакционная база данных 3-элементных наборов в нормализованном виде

Элементы	$i_2 i_3 i_4$	$i_2 i_3 i_5$	$i_2 i_3 i_8$	$i_3 i_4 i_5$	$i_3 i_4 i_8$	$i_3 i_5 i_8$	$i_4 i_5 i_8$
Значения	онлайн фото альбом	онлайн фото рамки	онлайн фото магазин	фото альбом рамки	фото альбом магазин	фото рамки магазин	альбом рамки магазин
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	1	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	1	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	1	0	0	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0
11	0	0	0	0	1	0	0
12	0	0	0	0	0	1	0
13	0	0	0	1	0	0	0
14	0	0	0	0	0	0	0
supp ($i_k i_j i_l$)	7.14	14.3	0	7.14	7.14	7.14	0
minsupp 28.6%							

Методика разработки семантического ядра сайта на основе алгоритма *Apriori*

Реализация двухэтапного анализа связей для поиска популярных наборов с помощью алгоритма *Apriori* и разработки АП на основе найденных популярных

наборов нашла свое отражение в аналитическом приложении *Deductor Academic*, версия 5.2, которого была использована для создания методики разработки СЯС.

Методику разработки СЯС можно представить в виде следующих шагов:

1) Формирование ТБД поисковых запросов с помощью средств статистики поисковых систем.

2) Конвертация ТБД поисковых запросов в текстовый формат.

3) Создание нового сценария в аналитическом приложении *Deductor Academic*.

4) Использование «Мастера импорта» для импорта ТБД в текстовом формате в приложение *Deductor*.

5) Использование «Мастера экспорта» для экспорта результатов обработки в текстовом формате.

6) Использование «Мастера обработки» для реализации «Ассоциативных правил», как одного из методов «Data Mining».

7) Формирование результирующей ТБД на основе текстового файла.

8) Перезапись атрибута *content* мета тэг *keywords* на основе результирующей ТБД.

Таблица 5.

Наборы-кандидаты в АП типа импликации $A \to B$

$itemset_2$	$itemset_1$	R	$A \to B$	$supp(A \to B)$, %	$conf(A \to B)$, %
$\{i_2\ i_3\}$ онлайн - фото	$\{i_2\}$ онлайн	$\{i_3\}$ фото	онлайн → фото	28.6	33
	$\{i_3\}$ фото	$\{i_2\}$ онлайн	фото →онлайн	28.6	80
$\{i_3\ i_4\}$ фото - альбом	$\{i_3\}$ фото	$\{i_4\}$ альбом	фото → альбом	28.6	100
	$\{i_4\}$ альбом	$\{i_3\}$ фото	альбом → фото	28.6	33
$\{i_3\ i_5\}$ фото - рамки	$\{i_3\}$ фото	$\{i_5\}$ рамки	фото → рамки	35.7	100
	$\{i_5\}$ рамки	$\{i_3\}$ фото	рамки →фото	35.7	41.6
$\{i_3\ i_8\}$ фото - магазин	$\{i_3\}$ фото	$\{i_8\}$ магазин	фото → магазин	28.6	100
	$\{i_8\}$ магазин	$\{i_3\}$ фото	магазин → фото	28.6	33

При этом термины «Мастер импорта», «Мастер обработки», «Ассоциативные правила», «Мастер экспорта» являются специфическими для приложения *Deductor* [3].

Предлагаемая методика была реализована для разработки СЯС типа Интернет-витрина Konica-Digital. При этом результат заключительного шага – формирование атрибута *content* мета тега *keywords*, будет выглядеть так: `<meta name="keywords" content="интернет магазин, магазин интернет, купить онлайн, фотографии онлайн, фотографии печать, фотографии рамки, магазин рамки интернет, купить онлайн рамки, ...">`.

Выводы

Реализация предлагаемой методики разработки СЯС с динамическим контентом позволила поднять позиции Konica-Digital в SERP на 25% для 70% информационных, 85% транзакционных и 60% нечетких запросов, вводимых пользователем в основные поисковые системы Yandex и Google. При этом в 1.5 раза сократились затраты рабочего времени специалиста по SEO, необходимые для достижения заявленных результатов.

Ограниченный объем статьи не позволил показать другие приложения методики разработки СЯС с динамическим контентом. Однако необходимо заметить, что при реализации предлагаемой методики для Интернет-магазина Vsedetali в качестве ТБД использовалась таблица заказов, а автоматизированное формирование атрибута *content* мета тэгов *keywords* на основе АП также позволило повысить полноту и точность, снизить время разработки семантического ядра сайта. Таким образом, предложенная методика разработки СЯС является достаточно универсальной, и с небольшими

доработками может быть применена для эффективного продвижения сайтов с динамическим контентом специалистами по SEO.

Список литературы

1. Ашманов И.С. Оптимизация и продвижение сайтов в поисковых системах / И.С. Ашманов, А.А. Иванов. – 3-е изд. – СПб. : Питер, 2011. – 463 с.
2. Как работают поисковые системы – сниппет, алгоритм обратных индексов, индексация страниц, особенности работы поисковиков [Электронный ресурс] / Режим доступа: http://ktonanovenkogo.ru/seo/search/kak-rabotayut-poiskovye-sistemy-snippet-index.html
3. Паклин Н.Б. Бизнес-аналитика: от данных к знаниям / Н.Б. Паклин, В.И. Орешков. – СПб.: Питер, 2009. – 624 с.
4. Chung D. Suchmaschinen-Optimierung: Der schnell Einstieg / D. Chung, A. Klünder. – Heidelberg : REDLINE/mitp, 2007. – 224 S.
5. Aden T. Google Analytics: Implementieren. Interpretieren. Profitieren. – Auflage: 2., aktualisierte und erweiterte Auflage. – München : Carl Hanser Verlag, 2010. – 463 S.
6. R. Agrawal, T. Imielinski, A. Swami. Mining Associations between Sets of Items in Massive Databases // Proc. of the ACM-SIGMOD 1993 Int'l Conference on Management of Data, Washington D.C., May 1993. – PP. 207-216.

РОЗРОБКА СЕМАНТИЧНОГО ЯДРА САЙТУ З ДИНАМІЧНИМ КОНТЕНТОМ НА ОСНОВІ АСОЦІАТИВНИЙ ПРАВИЛ

О.О. Арсірій, О.О. Ігнатенко, О.О. Леус

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

В результаті аналізу проблем просування в пошукових системах веб-ресурсів з динамічним контентом запропонована методика розробки семантичного ядра сайту на основі створення асоціативних правил за допомогою алгоритму пошуку популярних наборів Apriori в транзакційній базі даних пошукових запитів. Застосування методики дозволило підвищити повноту і точність, а також знизити час розробки семантичного ядра сайту типу Інтернет-вітрини та магазину.

Ключові слова: пошукова система, пошукові запити, семантичне ядро сайту, популярні набори, асоціативні правила, алгоритм Apriori

DEVELOPMENT OF A SEMANTIC CORE OF A WEB-SITE WITH DYNAMIC CONTENT BASED ON ASSOCIATION RULES

Elena A. Arsiry, Olga A. Ignatenko, Alexei A. Leus

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

In consequence of an analysis of promotion problems of web sites with dynamic content in the search engines a methodology of development of a web-site's semantic core was proposed namely through the association rules creation by using the search of popular sets in the transactional search queries' database – algorithm Apriori. Application of the methodology has allowed to improve the completeness and accuracy, and reduce the time on the development of a semantic core for such web-sites as an Internet-showcase and shop.

Keywords: search engine, search queries, semantic core of a web-site, popular sets, association rules algorithm Apriori

УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 1, pp. 87-93

ЗАХИСТ ВЕБ-СЦЕНАРІЇВ ВІД НЕСАНКЦІОНОВАНОГО КОПІЮВАННЯ І МОДИФІКАЦІЇ

Л.М. Тимошенко[1], **Ю.М. Чайківська**[2]

[1] Одеський національний політехнічний університет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: lmt0902@gmail.com
[2] Тернопільський національний педагогічний університет ім. В. Гнатюка,
вул. М.Кривоноса, 2, Тернопіль, 46027, Україна

Розглядаються системи захисту веб-сценаріїв, що дозволяють виявити зловмисні коди і захистити веб-сайти від копіювання інформації шляхом фільтрації даних. Побудовані інструменти з використанням механізму BEEP в браузерах дозволяють спростити застосування політики безпеки у веб-сценаріях, причому зміна мережевих сервісів вимагає мінімальних зусиль.

Ключові слова: політика безпеки, веб-сценарій, механізм BEEP, функція відслідковування

Постановка проблеми

Система захисту повинна бути багаторівневою і будуватися відповідно до необхідного рівня стійкості системи в цілому. Для надійного захисту необхідно розподілити функції між цими рівнями так, щоб здійснювалося дублювання функцій захисту і відбувалася компенсація недоліків одного рівня іншим. Криптографічний захист потрібно забезпечувати на всіх верхніх рівнях, проте його застосування має відповідати передбачуваним загрозам. Оскільки загальні витрати на захист великі, то в першу чергу потрібно підсилити його слабкі елементи.

Аналіз слабких місць при скануванні на мережевому рівні допоможе виявити серйозні недоліки, зокрема неправильно сконфігуровані міжмережеві екрани або вразливості веб-сервера, які можуть спровокувати потенційну загрозу і дозволити зловмисникам проникнути в систему захисту. Сканування на мережевому рівні забезпечує швидкий і детальний аналіз мережевої інфраструктури організації як ззовні, так і зсередини.

Аналіз останніх досліджень і публікацій

Найбільш небезпечними є вразливості проектування, які виявляються та усуваються з великими труднощами. Вразливість притаманна алгоритму, тому навіть досконала його реалізація не дозволяє уникнути закладеної загрози. Імітація атак не завжди можна реалізувати. Такі випадки можна розділити на дві категорії: ситуації, в яких програма призводить до відмови в обслуговуванні вузла або мережі, і ситуації, в яких не може проводитись атака в мережі. В цьому випадку можна скористатися системою аналізу захищеності на рівні операційної системи, агенти якої встановлюються на кожен контрольований вузол і проводять всі перевірки локально. Для вирішення цієї проблеми деякі компанії-виробники пропонують користувачам декілька систем аналізу захищеності, що працюють на всіх вказаних вище рівнях − мережевому, системному і прикладному. Сукупність цих систем дозволяє з високим ступенем ефективності

визначити майже всі відомі вразливості.

Зокрема, компанія Internet Security Systems пропонує сімейство *SAFEsuite*, що складається з чотирьох сканерів: *Internet Scanner*, *System Scanner*, *Security Manager* і *Database Scanner* [1]. На сьогоднішній день це єдина компанія, яка пропонує системи аналізу захищеності, що функціонують на всіх трьох рівнях інформаційних інфраструктур. Інші компанії пропонують два або один сканер (*Network Associates*, *NetSonar* та ін.) [2].

Компанія Cisco пропонує тільки систему аналізу захищеності на рівні мережі і поділяє всі вразливості на два класи: потенційні, що випливають з перевірок заголовків і так званих активних «підштовхувань» (nudge) сервісу або аналізованого вузла. Потенційна вразливість може існувати в системі, проте активні перевірки зондування не підтвердять її; підтверджені − виявлені та існуючі на аналізованому хості.

Відмінність між системами *CyberCop Scanner* і *Internet Scanner* полягає в тому, що розробники з NAI не додають в свою систему перевірку, якщо не впевнені у її ефективності. В той же час розробники ISS це роблять навіть тоді, коли перевірка знаходить вразливість з певною точністю. Після випуску системи відбувається повернення до розроблених перевірок, їх покращення, додавання нових механізмів здійснення перевірок для підвищення достовірності. Не всі перевірки, розроблені в лабораторіях, функціонують належним чином. На це можуть впливати такі фактори:

- особливості конфігурації системи користувача;
- метод, яким було скомпільовано домен або сервіс;
- помилки віддаленої системи та інше.

В таких випадках автоматична перевірка може пропустити вразливість, яка легко визначається вручну і може бути широко розповсюджена у багатьох системах.

Мета дослідження

Мережевий сканер повинен бути першим інструментом, що використовується у процесі аналізу захищеності сценаріїв і повинен забезпечувати швидкий огляд загроз, які потребують уваги. Для забезпечення захисту від модифікацій веб-сценаріїв необхідно запропонувати механізм вбудованої політики безпеки в браузері.

Основна частина

Мережа складається із каналів зв’язку, вузлів, серверів, робочих станцій, прикладного і системного програмного забезпечення, баз даних і т.д. Всі ці компоненти потребують оцінки ефективності їхнього захисту. Засоби аналізу захищеності аналізують мережу і здійснюють пошук «слабких» місць, обробляють отримані результати і створюють різного роду звіти. До проблем, що ідентифікуються системами аналізу захищеності, належать:

- «люки» в програмах (*back-door*) і програми типу «троянський кінь»;
- «слабкі» паролі;
- чутливість до проникнення з незахищених систем;
- неправильне налаштування мережевих екранів, веб-серверів і баз даних та ін.

Технологія аналізу захищеності є дієвим методом реалізації політики мережевої безпеки проти порушення ззовні або зсередини мережі.

Веб-вузли, які дозволяють переглядати сторінки, зазвичай фільтрують інформацію для попередження проникнення коду сценарію в запущені браузери з різними алгоритмами, що ускладнює процес фільтрування і захисту від атак. Можна запропонувати альтернативний механізм для уникнення внесення сценарію в браузер − це вбудована політика безпеки в браузері. Ідея полягає в тому, що у веб-сайт вбудовується система

захисту, що дозволяє визначити, які сценарії запущені і коли. В такому випадку браузер зможе керувати сценарієм.

Багато веб-сайтів перевидають контент, що змінюється групами користувачів або іншим чином, наприклад, рекламною мережею і пошуковими системами. Якщо перевиданий контент містить вбудовані сценарії, відвідувачі сайту можуть бути не захищені від атак типу «перехресний сценарій сайту» (cross-site scripting (XSS)) [3]. Це дозволить сайту виступити в ролі учасника атаки на інші сайти. Стандартним захистом для веб-сайтів є фільтр або модифікація контента, видалення вбудованих сценаріїв або інших потенційно-небезпечних елементів [4].

На практиці реалізація фільтрування є складною задачею. Представлення інформації на сайтах потребує збільшення контенту із зображеннями, гіперпосиланнями, стилями типографічного оформлення і т.д. У сценарій може бути вкладений контент різними шляхами і можливо блокувати скрипти без виведення з ладу контентів. Однією із причин несанкціонованого копіювання є те, що різні структурний аналіз браузерів і візуалізація контенту: для одного фільтрування може бути ефективним, а для іншого ні. Окрім того, аналіз і спотворення відображення контенту використовують сучасні атаки, що обходять фільтри сервера (наприклад, черв'як Сема і Яманера) [5]. Запропонований метод для запобігання ін'єкції зловмисного скрипта базується на двох аспектах:

1) браузери формують механізм виявлення сценарію; якщо браузер не аналізує контент як скрипт в той час, як відображає веб-сторінку, то він не буде виконуватися;

2) розробник веб-програм повинен знати, які сценарії потрібно виконувати для того, щоб програма була функціональною.

Перший аспект ґрунтується на тому, що браузер − це найкращий варіант для фільтрації сценаріїв. Насправді більшість веб-сервісів (наприклад, GPokr, S3AjaxWiki) логічно виконуються в браузері з активними веб-сайтами як накопичення даних. Фільтрування з боку браузера може бути єдиним варіантом для цих сервісів.

Другий аспект ґрунтується на тому, що веб-сайт повинен забезпечувати політику фільтрації для браузера. Тобто він може конкретизувати, який сценарій прийняти до виконання, а який відмінити. Таким чином, веб-сайт встановлює політику безпеки і браузер надає інструкції для її виконання. Такий метод називається вбудованою політикою безпеки в браузері – *Browser-Enforced Embedded Policies* (BEEP).

Розглянутий метод BEEP дозволяє управляти генеральною політикою безпеки. Захист політики реалізований за допомогою довіреної функції JavaScript, що дозволяє вбудувати перегляд веб-сторінки. Цю функцію називають «гаком» (відслідковуванням). Відповідно модифікований браузер передає кожен сценарій, що виявляється за допомогою «гака» при структурному аналізі (разом з іншою суттєвою інформацією), і сценарій виконується у випадку, якщо функція «гака» надасть дозвіл.

В результаті дослідження була додана підтримка BEEP до кількох браузерів і побудовані інструменти, що дозволяють спростити застосування політики безпеки у веб-сценарії. Було виявлено, що підтримка BEEP в браузерах вимагає невеликих і локалізованих модифікацій, а зміна мережевих сервісів вимагає мінімальних зусиль.

Розглянемо переваги методу BEEP. По-перше, це гнучка політика безпеки. «Гаком» безпеки може бути будь-яка функція, що реалізується за допомогою JavaScript. Можна розглянути два види політик безпеки. Перший − рекомендований список, в якому функція «гака» включає в собі односторонню хеш-функцію кожного легітимного сценарію, розташованого на сторінці. При виявленні небезпечного сценарію в браузері він передається функції «гака», яка здійснює хешування сценарію і порівнює його з рекомендованим списком. У випадку, коли хешований сценарій не знайдено у списку, він відкидається. Другий тип політики безпеки полягає у використанні механізму захисту об'єктної моделі документів (DOM), що забезпечує стандартний інтерфейс для доступу і керування HTML-об'єктами. В даному випадку веб-сервіси структурують сторінки для ідентифікації контенту, що може містити зловмисні сценарії. Можливий

зловмисний контент користувача розміщений в або елементах, що виконують роль механізму захисту аплетів (*sandbox*). Наприклад: . . .можливий зловмисний контент. . . .

В межах *sandbox* дозволено використовувати великий контент, що може містити типографічні стилі, графічні зображення та ін., проте всі ці сценарії блоковані до виклику функції «гака». При виклику функції «гака» здійснюється тестування документа в проаналізованому відображенні дерева DOM. Починаючи з вузла сценарію DOM-функція «гака» ретельно досліджує всі вузли аж до кореня дерева, шукаючи «не виконувані» (noexecute) вузли. Якщо такий вузол знайдено, сценарій не виконуватиметься.

Поряд з механізмами безпеки, що включать в собі рекомендований список і DOM-аплет, BEEP дозоляє виявити і відфільтрувати всі ін'єктовані сценарії. По-перше, перевірені сценарії ідентифікуються безпосередньо веб-сторінкою, по-друге, браузер запускає функцію «гака» перед виконанням будь-якого сценарію. В цьому можна легко переконатися: визначення функції гака як першого сценарію в заголовку документа гарантує те, що він буде аналізуватися першим. Разом ці умови означають, що будь-який не схвалений сценарій буде відкинуто перед його запуском.

Описаний метод потребує модифікацій браузера. Наприклад, в місцях, де відбувається модифікація браузера, потрібно встановити в початковому коді виклик інтерпретатора JavaScript. В цих точках виклику браузер ідентифікує сценарій веб-сторінки. Для того, щоб застосувати функцію «гака», потрібно спочатку вставити коди в програму і викликати інтерпретатор JavaScript.

В залежності від результату виконання першої функції програми потрібно запустити сценарій із сторінки або пропустити його. Для проведення дослідження були модифіковані Konqueror і Safari браузери для підтримки функції «гака» і реалізовано часткову підтримку закритого коду веб-браузера Opera. Ці зміни вимагають близько 650 стрічок коду в першому випадку і близько 100 стрічок для Opera.

Атаки, що базуються на використанні зловмисного сценарію, написаного на JavaScript, вбудовують його код в контент довіреного веб-вузла. При перегляді користувачем сторінки сайту вбудований сценарій завантажується і виконується в браузері користувача з привілеями довіреного сайту. Ін'єктований сценарій може видавати привілейовану інформацію (cookies, історія браузера, приватна інформація з сайту) [6]. Сценарій може використовувати браузер користувача для реалізації атаки відмови служб на веб-вузлі і т.п.

Проникнення сценарію може здійснюватися кількома шляхами. В перехресному сценарії сайту (XSS) атакуючий використовує веб-сайти, вносячи підготовлений користувачем текст в сторінки без фільтрування тексту. Наприклад, члени онлайн-товариства типу MySpace, Blogger, і Flickr можуть увійти у власний контент і додавати коментарі в інші контенти [6]. Цей контент зберігається на сайті і будь-хто може його переглянути. Якщо зловмиснику вдалося включити свій скрипт в цей контент, то будь-які читачі цього контенту будуть запускати скрипт з привілеями сайту. Якщо читач є членом сайту, скрипт може мати доступ до модифікації читацького контенту, включаючи приватну інформацію, що зберігається на сайті або в браузері (рис. 1).

Інший метод проникнення сценарію − «віддзеркалення». Наприклад, при запиті неіснуючої сторінки багато сайтів намагаються представити корисну відповідь, що включає URL неіснуючої сторінки. Тому, якщо сайт не захищений, програма <script>...</script> в URL виконуватиметься в браузері користувача, коли він отримає повідомлення «сторінку не знайдено». Таким чином зловмисник намагається заманити користувача на URL з вбудованими сценаріями. Наприклад: http://trusted.site/<script>document.location='http://evil.site/?'+document.cookie</script>.

Зловмисник може розмістити URL як спам в електронній пошті, а також в коментарях або рекламі на trusted.site чи іншому сайті. Якщо жертва завантажує посилання, сценарій виконуватиметься на незнайденій сторінці, що обслуговується

`trusted.site`, вилучаючи cookie користувача і надсилаючи його на `evil.site`.

Інший можливий сценарій атаки використовує динамічну природу JavaScript санкціонованого доступу до веб-сторінок, де HTML-контент обслуговується веб-сервером і змінюється в браузері через виконання сценаріїв. Наприклад, сайт можна побудувати таким чином, що URL типу `http://vulnerable.site/welcome.html?name=Joe` буде видавати персоналізований контент, використовуючи статичну HTML сторінку в поєднанні з вбудованим сценарієм. Зокрема, сценарій може використовувати особливості типу innerHTML і document.write для модифікації контенту сторінки, що відображається в браузері, таким чином персоналізуючи значення «name». Це дає можливість зловмисному сценарію проникнути в браузер за допомогою комбінації «name».

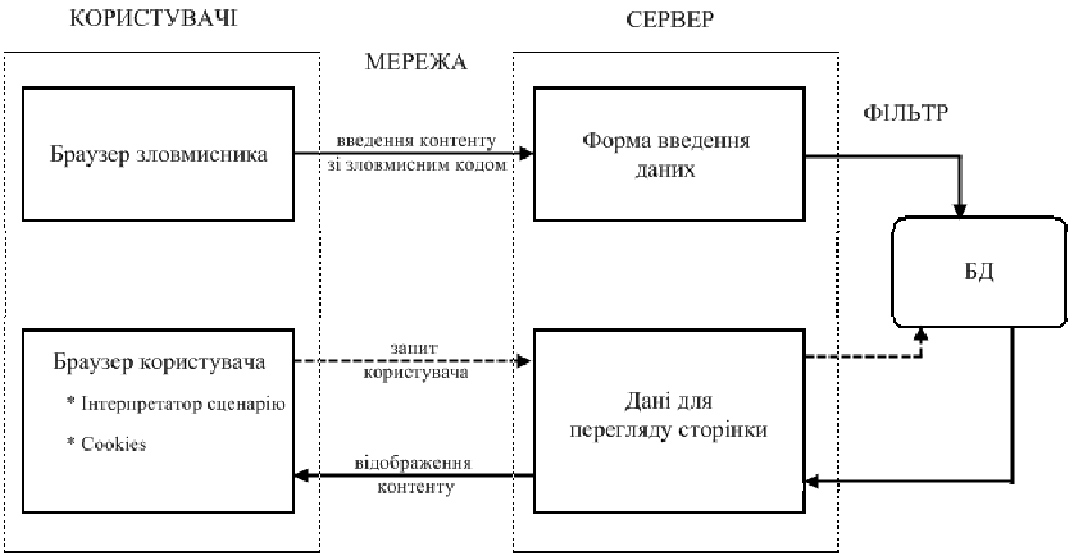

Рис. 1. Схема виявлення ін'єктованих сценаріїв

Стандартним вирішенням проблеми проникнення сценарію є встановлення фільтру на веб-вузлі або перетворення всіх можливих зловмисних контентів в сценарії для видалення або блокування.

Для виявлення вбудованих сценаріїв можна запропонувати альтернативний підхід, ідея якого полягає в конкретизації кожної сторінки веб-вузла, політика безпеки якого дозволяє або забороняє виконання сценарію. В даному випадку веб-вузол конкретизує політику через «гак» безпеки, що використовується для перевірки сценарію перед його виконанням у браузері. Функція гака реалізує ефективний захист - будь-який сценарій підлягає детальному аналізу перед його виконанням. Це здійснюється наступним чином: функція інсталюється перед аналізом зловмисного коду і його виконанням. Стандарт HTML не конкретизує порядок аналізу і виконання. На практиці перевірено, що в основному браузери аналізують і виконують перший елемент `<script>` в заголовку. Поведінка браузера залежить від визначення функції «гака» в першому сценарії елемента `<head>` в документі. Таким чином, жодний динамічний контент не включається доти, поки не виконається функція «гака» в `<head>` кожної веб-сторінки. Варто зазначити, що введення функції захисту відразу захищає від невмілого користування, бо будь-які зловмисні коди, спрямовані на зміну функції, будуть проаналізовані після встановлення. Таким чином здійснюється фільтрування «гаком» і попередження запуску програм.

Для перевірки політики безпеки від модифікації сценарію був використаний тест, що містить комплект 61 векторних атак XSS [7]. Тест перевіряє частини коду HTML і JavaScript, що можуть бути вбудовані в контент користувача. Нами було обрано 26 сайтів, які були локально збережені, щоб не вносились зміни з боку мережі. В подальшому використовувався сценарій ідентифікації для обчислення функції SHA-1 кожного сценарію в межах сторінки. Кожна сторінка 26 сайтів була завантажена в браузері на протязі 20 годин і вимірювався загальний час завантаження кожної сторінки: для не модифікованих 520 сторінок час складав 698.2 секунди, а для сторінок, що містять вбудовану політику безпеки, − 798.6 секунд. Отже, в середньому час завантаження збільшився на 14.4%.

Висновки

Запропонований механізм підтримки політики безпеки BEEP застосовано до кількох браузерів, що дозволило посилити захист у веб-сценаріях. Він забезпечує захист веб-сценарію від модифікації, використовуючи функцію «гака», що включає в собі односторонню хеш-функцію кожного легітимного сценарію, розташованого на сторінці.

Варто зазначити, що цих механізмів вистачає для виявлення зловмисного сценарію, проте можна додавати й інші механізми. Наприклад, функція «гака» може використовуватися для перевірки веб-сайту і видачі повідомлення про знаходження зловмисного сценарію. Проте механізми політики безпеки можуть змінюватися через певний час: нова політика безпеки дописується до сторінки сайту і буде призначатися браузером.

Список літератури

1. Shriram Krishnamurthi. The Continue server (or, How I Administered PADL 2002 and 2003) // Lecture Notes in Computer Science. – 2003. – Vol.2562. – PP. 2-16.
2. Antonatos S. Puppetnets: Misusing Web Browsers as a Distributed Attack Infrastructure / S. Antonatos, P. Akritidis, V.T. Lam, K.G. Anagnostakis // ACM Transactions on Information and System Security. – 2008. – Vol.12, Iss.2. – PP. 1-38.
3. Klein A. DOM Based Cross Site Scripting or XSS of the Third Kind *[Електронний ресурс]* // Web Application Security Consortium. – Режим доступу: http://www.webappsec.org/projects/articles/071105.shtml.
4. Bowman M.C. et al. The Harvest Information Discovery and Access System // Computer Networks and ISDN Systems. – 1995. – Vol.28, Iss.1-2. – PP. 119-125.
5. Castillo C. Cooperation Schemes between a Web Server and a Web Search Engine / C. Castillo // LA-WEB'03 Proceedings of the First Conference on Latin American Web Congress. – USA: IEEE Computer Society, 2003. – PP. 212-213.
6. Srinivasan P., Pant G., Menczer F. Target Seeking Crawlers and their Topical Performance *[Електронний ресурс]* / P. Srinivasan, G. Pant, F. Menczer. – Режим доступу: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.23.6092.
7. RSnake. XSS (Cross Site Scripting) Cheat Sheet Esp: for filter evasion. http://ha.ckers.org/xss.html.

ЗАЩИТА ВЕБ-СЦЕНАРИЕВ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ И МОДИФИКАЦИИ

Л.Н. Тимошенко[1], Ю.М. Чайковская[2]

[1] Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: lmt0902@gmail.com
[2] Тернопольский национальный педагогический университет имени В. Гнатюка,
ул. М. Кривоноса, 2, Тернополь, 46027, Украина

Рассмотрены системы защиты веб-сценариев, которые дают возможность обнаружить злоумышленные коды и защитить веб-сайты от копирования информации путем фильтрации данных. Разработанные инструменты с использованием механизма BEEP в браузерах позволяют упростить применение политики безопасности в веб-сценариях, причем смена сетевых сервисов требует минимальных усилий.
Ключевые слова: политика безопасности, веб-сценарий, механизм BEEP, функция отслеживания

PROTECTION OF WEB SCRIPTS FROM UNAUTHORIZED COPYING AND MODIFICATION

Lidiya M. Tymoshenko[1], Julia M. Chaikivska[2]

[1] Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: lmt0902@gmail.com
[2] Ternopil V. Hnatyuk National Pedagogical University,
2 M. Kryvonosa str., Ternopil, 46027, Ukraine

We consider the protection systems of web scripts that allow detecting malicious code and making possible protection websites from unauthorized copying information by filtering the data. The developed tools (with the use of BEEP in browsers) allow to simplify the application of security policies in a web scripts. In addition, changes of network services for using proposed methods require minimal effort.
Keywords: security policy, web script, BEEP, tracking feature

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 2, номер 1, 2012. Одеса – 94 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 2, номер 1, 2012. Одесса – 94 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 2, No. 1, 2012. Odesa – 94 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 №8 від 26.04.2011)

Адреса редакції: Одеський національний політехнічний університет,

проспект Шевченка, 1, Одеса, 65044 Україна

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

E-mail: immm.ukraine@gmail.com