

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 3, № 3

Volume 3, No. 3

Одеса – 2013  
Odesa – 2013

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

**Виходить** 4 рази на рік

**Заснований** Одеським національним  
політехнічним університетом у 2011 році

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

**Головний редактор:** *Г.О. Оборський*

**Заступник головного редактора:**

*А.А. Кобозєва*

**Відповідальний редактор:** *І.І. Бобок*

**Редакційна колегія:**

*Т.О. Банах, П.І. Бідюк, Н.Д. Вайсфельд,*

*А.Ф. Верлань, О.Ф. Дащенко, В.Б. Дудикевич,*

*Л.Є. Євтушик, М.П. Карпінський,*

*М.Б. Копитчук, С.В. Ленков, Є.В. Малахов,*

*І.І. Маракова, А.Д. Мілка, С.А. Нестеренко,*

*М.С. Никитченко, С.А. Положаєнко,*

*О.В. Рибальський, В.Д. Русов, І.М. Ткаченко,*

*А.В. Усов, С.В. Філіппова, В.О. Хорошко,*

*М.Є. Шелест, М.С. Яджак*

**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*

**Editorial Board:**

*T. Banakh, P. Bidyuk, A. Daschenko,*

*V. Dudykevich, L. Evtushik, S. Filippova,*

*V. Horoshko, M. Karpinski,*

*N. Kopytchuk, S. Lenkov, E. Malakhov,*

*I. Marakova, A. Milka, S. Nesterenko,*

*N. Nikitchenko, S. Polozhaenko, V. Rusov,*

*O. Rybalsky, M. Shelest, I. Tkachenko, A. Usov,*

*N. Vaysfeld, A. Verlan, M. Yadzhak*

**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](mailto: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](mailto:immm.ukraine@gmail.com)

© **Одеський національний політехнічний університет, 2013**

---

## ЗМІСТ / CONTENTS

---

- СТРУКТУРНЕ ТЕСТУВАННЯ  
ПРОГРАМНИХ СИСТЕМ З  
ВИКОРИСТАННЯМ ЕЛЕМЕНТІВ  
КОМП'ЮТЕРНОЇ АЛГЕБРИ  
Л.С. Ломакіна, А.М. Вігура
- 201 STRUCTURAL TESTING OF  
SOFTWARE SYSTEMS USING  
ELEMENTS OF COMPUTER ALGEBRA  
Lomakina L., Vigura A.
- ВИЗНАЧЕННЯ ОПТИМАЛЬНИХ  
ПАРАМЕТРІВ ТЕХНІЧНОГО  
ОБСЛУГОВУВАННЯ ЗА СТАНОМ  
СКЛАДНИХ ОБ'ЄКТІВ  
РАДІОЕЛЕКТРОННОЇ ТЕХНІКИ  
С.В. Ленков, О.В. Селюков,  
В.В. Зубарев, В.М. Цицарев
- 215 DETERMINATION OF THE OPTIMAL  
PARAMETERS OF MAINTENANCE AS  
FOR THE CONDITION OF COMPOUND  
FACILITIES OF RADIO ELECTRONIC  
EQUIPMENT  
Lenkov S., Selyukov O., Zubarev V.,  
Tsytaryev V.
- СТРУКТУРОВАНІСТЬ СИГНАЛОГРАМ  
ТА УНІВЕРСАЛЬНІСТЬ  
ФРАКТАЛЬНОГО ПІДХОДУ ПРИ  
СТВОРЕННІ ІНСТРУМЕНТАРІЮ  
ФОНОСКОПІЧНИХ ЕКСПЕРТИЗ  
В.В. Журавель, О.В. Рибальський,  
В.І. Соловійов
- 225 SIGNALOGRAMM STRUCTURE AND  
UNIVERSALITY OF THE FRACTAL  
APPROACH TO THE DEVELOPMENT  
OF THE PHONOSCOPE ASSESSMENT  
TOOLKIT  
Zhuravel V., Rybalsky O., Solovyev V.
- МЕТОДИЧНІ ЗАСАДИ  
ЗАСТОСУВАННЯ НЕЙРОМЕРЕЖ У  
ЗАДАЧАХ ПРОГНОЗУВАННЯ ТА  
КЕРУВАННЯ  
С.В. Ленков, В.М. Штепа, А.О. Дудник,  
А.С. Шворов
- 233 METHODOLOGICAL BASIS OF  
NEURAL NETWORKS APPLICATIONS  
FOR FORECASTING AND  
MANAGEMENT TASKS  
Lenkov S., Shtepa V., Dudnik A.,  
Shvorov A.
- ІНФОРМАЦІЙНА КОГНІТИВНА  
МОДЕЛЬ ТЕХНОЛОГІЧНОЇ  
ВЗАЄМОЗАЛЕЖНОСТІ СУДНОВИХ  
ТЕХНІЧНИХ ЗАСОБІВ  
Н.Д. Рудніченко, В.В. Вичужанін
- 240 INFORMATION COGNITIVE MODEL  
OF TECHNOLOGICAL  
INTERDEPENDENCE OF MARINE  
TECHNICAL RECOURSES  
Rudnichenko N., Vichuzhanin V.

ПІДВИЩЕННЯ ПРИХОВАНОЇ  
ПРОПУСКНОЇ СПРОМОЖНОСТІ  
СТІЙКИХ ДО СТИСКУ  
СТЕГАНОГРАФІЧНИХ АЛГОРИТМІВ  
ДЛЯ ДОВІЛЬНИХ ЗОБРАЖЕНЬ-  
КОНТЕЙНЕРІВ  
М.О. Мельник

248 INCREASE STEGANOGRAPHIC  
CAPACITY OF COMPRESSIVE  
STRENGTH ALGORITHMS FOR  
ARBITRARY COVER IMAGES  
Melnik M.

МОДЕЛЮВАННЯ ПРОЦЕСІВ  
ПРИПИНЕННЯ ГОРІННЯ МЕТОДОМ  
КЛІТИННИХ АВТОМАТІВ  
М.О. Пустовіт

258 MODELING THE PROCESSES OF  
BURNOUT BY CELLULAR  
AUTOMATA  
Pustovit M.

АЛГОРИТМИ ОПРАЦЮВАННЯ  
ІНФОРМАЦІЙНИХ ПОТОКІВ В  
КОМП'ЮТЕРНИХ СИСТЕМАХ  
І.З. Якименко, М.М. Касянчук,  
Л.М. Тимошенко, Н.Є. Гребень

266 ALGORITHMS OF PROCESSING OF  
INFORMATION FLOWS IN  
COMPUTER SYSTEMS  
Yakimenko I., Kasyanchuk M.,  
Timoshenko L., Greben N.

АНАЛІЗ ПЕРЕВАГ ПРОСТОРОВОЇ  
ОБЛАСТІ ЦИФРОВОГО  
ЗОБРАЖЕННЯ-КОНТЕЙНЕРА ДЛЯ  
СТЕГАНОПЕРЕТВОРЕННЯ  
О.В. Костирка

275 ANALYSIS ON THE BENEFITS OF  
SPATIAL DOMAIN OF COVER IMAGE  
FOR STEGANOGRAPHY  
TRANSFORMATION  
Kostyrka O.

СИГНАЛИ СИНХРОНИЗАЦІЇ У  
МЕРЕЖАХ З КОМУТАЦІЄЮ  
ПАКЕТІВ.  
КОНТРОЛЬ І ВИМІР ЇХ ПАРАМЕТРІВ  
Н.В. Федорова

283 SYNCHRONIZATION SIGNALS IN  
PACKET SWITCHED NETWORKS:  
PARAMETER MONITORING AND  
MEASUREMENT  
Fedorova N.

ІНТЕРАКТИВНІ КОМУНІКАТИВНІ  
ТЕХНОЛОГІЇ ОСВІТИ: МОБІЛЬНЕ  
НАВЧАННЯ ЯК НОВА ТЕХНОЛОГІЯ  
В ПІДВИЩЕННІ МОВНОЇ  
КОМПЕТЕНЦІЇ СТУДЕНТІВ  
НЕМОВНИХ ВНЗ  
О.В. Мардаренко

288 INTERACTIVE COMMUNICATION  
TECHNOLOGIES IN EDUCATION:  
MOBILE LEARNING AS A NEW  
TECHNOLOGY OF IMPROVING OF  
LANGUAGE COMPETENCE OF NON-  
LINGUISTIC UNIVERSITY STUDENTS  
Mardarenko E.

# СТРУКТУРНОЕ ТЕСТИРОВАНИЕ ПРОГРАММНЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ЭЛЕМЕНТОВ КОМПЬЮТЕРНОЙ АЛГЕБРЫ

Л.С. Ломакина, А.Н. Вигура

Нижегородский государственный технический университет им. Р.Е. Алексеева,  
ул. Минина, 24, Нижний Новгород, 603950, Российская Федерация; e-mail: llomakina@list.ru

Предложен метод структурного тестирования программных систем, основанный на алгебраической модели программы и динамическом символьном выполнении на уровне машинного кода и позволяющий автоматизировать модульное тестирование программ, реализованных на компилируемых языках программирования.

**Ключевые слова:** программные системы, тестирование, генерация тестовых данных, алгебраическая модель, символьное выполнение

## Введение

В настоящее время актуальной является проблема контроля и обеспечения надежности программных систем. Как известно, надежность любой вычислительной системы обусловлена двумя факторами – надежностью аппаратного обеспечения и надежностью программ, управляющих аппаратным обеспечением. При этом, хотя для диагностирования аппаратных средств разработаны эффективные методы, позволяющие выявлять дефекты и формально обосновывать их отсутствие, аналогичная задача для программ в полной мере не решена. Постоянное усложнение используемых на практике в различных отраслях промышленности программных систем привело как в области верификации и тестирования, так и в области синтеза надежных и контролепригодных программ.

Основной проблемой тестирования является принципиальная невозможность нахождения всех дефектов в программном продукте. Как следствие, при тестировании требуется решение следующих взаимосвязанных задач:

- 1) определение полноты тестирования;
- 2) выбор множества тестовых воздействий с целью обеспечения заданной полноты тестирования;
- 3) проверка корректности полученных выходных данных.

При этом несомненно актуальной является задача снижения общих затрат на тестирование и поддержку программного продукта. Одним из путей к решению данной задачи является обнаружение дефектов на ранних стадиях жизненного цикла программной системы, реализуемое с помощью автоматизации тестирования на этапе разработки и мониторинга метрик качества в рамках систем непрерывной интеграции.

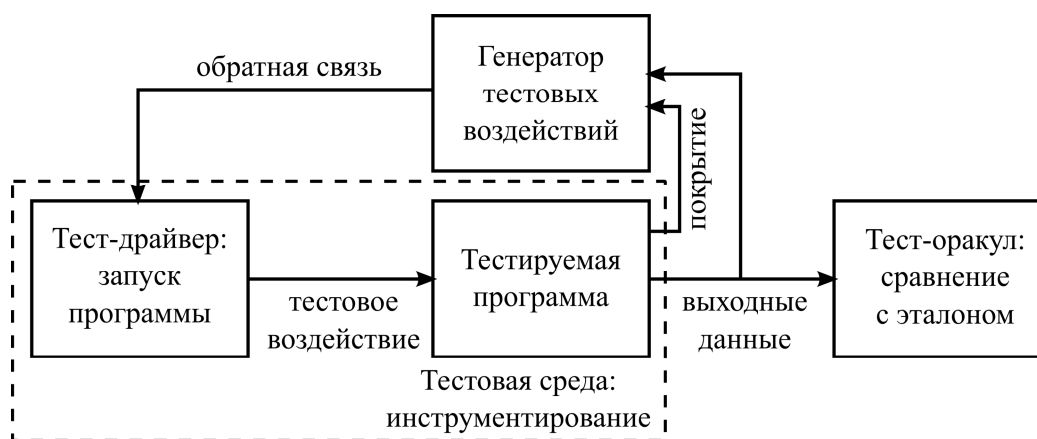
Тестирование на этапе разработки представляет собой структурное тестирование, в рамках которого тесты выбираются исходя из граф-модели программной системы, а в качестве метрики качества используется тестовое покрытие кода. В силу этого далее в настоящей работе рассматривается структурное тестирование. Отметим, что на практике полной автоматизации поддаются только модульные тесты, в то время как интеграционное дизайн-тестирование выполняется вручную разработчиками. При этом

тестовые воздействия, выбранные для модульного тестирования, зачастую тоже выбираются разработчиками вручную. Это приводит к существенным затратам времени на тестирование и, соответственно, к повышению затрат на разработку и стабилизацию программного продукта. Таким образом, актуальной является задача разработки методов и реализующих их программных средств, ориентированных на автоматическую оценку полноты тестирования и автоматизированный выбор тестовых воздействий.

Современные подходы (реализованные, в частности, в системах CUTE и CREST [1]) к автоматизации тестирования ориентированы на генерацию тестовых данных и основаны на динамическом символьном выполнении, при котором одновременно производится выполнение программы «в числах» и «в символах», и численные значения данных используются в том случае, когда символьные не могут быть определены. Отметим, что существующие системы не позволяют обрабатывать в символьном виде операции разыменования указателей, что ограничивает их применимость, а также не поддерживают обработку взаимодействия инструментируемого и неинструментируемого кода (например, стандартных подпрограмм). Настоящая работа нацелена на преодоление указанных недостатков. В работе предложен метод модульного тестирования программных систем, основанный на динамическом символьном выполнении на уровне машинного кода и алгебраической модели программы, и позволяющий учитывать в модели операции над указателями, а также обрабатывать вызовы стандартных подпрограмм. На основе предложенного метода разработана программная система, реализующая контролируемое выполнение программы с помощью доработанной виртуальной машины Valgrind [2].

## Основная часть

Структурное тестирование предполагает выбор тестовых воздействий на основе граф-модели программы таким образом, чтобы достичь желаемого значения тестового покрытия (например, покрытия дуг управляющего графа). Общая схема структурного тестирования приведена на рис. 1.



**Рис. 1.** Схема структурного тестирования

Отметим, что как генерация тестовых данных, так и определение тестового покрытия требуют модификации тестируемой программной системы, поскольку в общем случае факты выполнения тех или иных блоков кода системы не являются

наблюдаемыми – данная проблема решается вставкой инструментального кода, выполняющего трассировку программы. Таким образом, чтобы реализовать динамическую генерацию тестовых воздействий, требуется решить следующие задачи:

1) Раскрытие структуры программной системы - построение ее модели структуры с целью дальнейшего выбора тестовых путей.

2) Модификация тестируемой программной системы – вставка инструментального кода, отслеживающего ход выполнения программы и операции с программными переменными.

3) Символьное выполнение программы – определение условий прохождения тестовых путей в зависимости от входных данных в символьном виде.

4) Выбор тестовых воздействий на основе полученных условий прохождения путей.

### Базовая модель программы

Нашей задачей является определение тестового воздействия для выбранного тестового пути, для чего нужно определить условие прохождения этого пути в зависимости от входных переменных в символьном виде (в виде алгебраического выражения). С целью решения данной задачи будем использовать алгебраическую модель программы в виде множества связанных по управлению блоков машинных инструкций [3], как показано на рис. 2.

Предлагаемая модель программы основана на понятии алгебраического выражения. Алгебраическое выражение [3] представляет собой один или несколько термов, соединенных между собой знаками операций и знаками последовательности операций (скобками). Множество выражений определим следующим образом:

$$Expr = Term \cup \{(o, a) : o \in Op, a \in Expr^{arity(o)}\},$$

где

$Expr$  — множество выражений;

$Term$  — множество термов;

$Op$  — множество возможных операций;

$arity: Op \rightarrow N$  — отображение, определяющее для каждой операции количество аргументов.

На уровне машинных инструкций ЭВМ оперирует рациональными числами – константами и располагающимися по определенным адресам в памяти переменных. Исходя из этого, определим множество термов следующим образом:  $Term = Q \cup Addr \times Types$ , где  $Addr \subset N \cup \{0\}$  – множество допустимых адресов,  $Types$  — множество примитивных типов данных

Инструкции представляют собой элементы следующего множества:

$$Ins = \{(addr, expr, bt, bf)\} \subseteq Addr \times Expr \times Addr \times Addr,$$

где

$Addr$  — множество допустимых адресов памяти,  $addr$  — адрес инструкции,  $expr$  — выполняемое выражение;

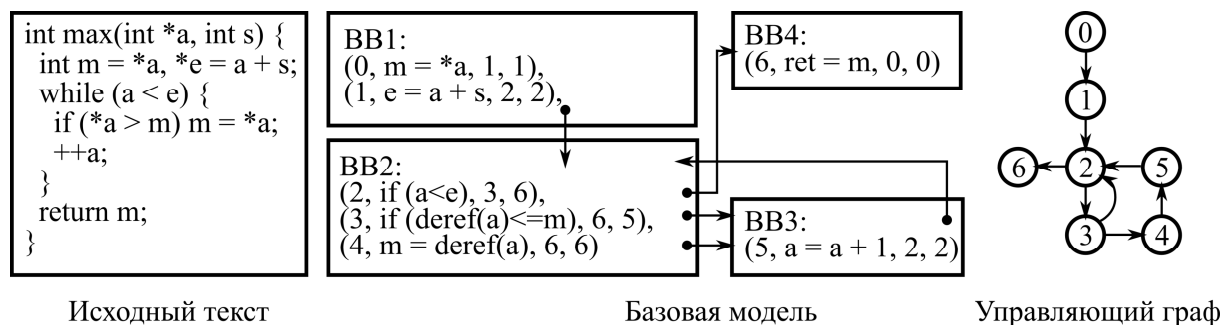
$bt$  — адрес следующей инструкции в случае истинности значения  $e$ ;

$bf$  — адрес следующей инструкции в случае ложности значения  $e$ .

Для ветвлений  $bt \neq bf$ , для прочих инструкций  $bt = bf$ . Множество  $Addr$  определяет допустимые адреса программных инструкций и переменных. Инструкции

сгруппированы в базисные блоки  $bb_i$ , составляющие множество  $BB \subseteq Ins^* = \bigcup_{i=0}^{\infty} Ins^i$ ,

каждый из которых представляет собой неделимую последовательность инструкций, в которой выделена только одна входная инструкция и существует не менее одной выходной инструкции, передающей управление на начало другого базисного блока. Выделив во всем множестве базисных блоков входной и выходной блоки, сформируем модель программы следующим образом. Обозначим адрес входного базисного блока через  $entry$ , а адрес выходного базисного блока через  $exit$ . Программу будем представлять в виде тройки  $P = (BB, entry, exit)$ .



**Рис. 2.** Базовая модель и управляющий граф программы

Построение модели будем осуществлять с помощью анализа машинного кода программы, что по сравнению с методами анализа программ, работающими с исходными текстами, дает следующие преимущества:

- отсутствие необходимости выполнения трудоемкого синтаксического анализа исходных текстов и учета индивидуальных особенностей различных компиляторов;
- отсутствие проблемы обработки взаимодействия инструментируемого и неинструментируемого кода в том случае, когда не все исходные тексты доступны (в частности, при вызовах подпрограмм стандартной библиотеки).

### Диагностическая модель

Для определения полноты тестирования и выбора тестовых воздействий будем использовать взвешенный управляющий граф программы (УГП) с детализацией до инструкций. Управляющий граф программы является одной из основных диагностических моделей в структурном тестировании программных систем. В УГП вершины соответствуют элементам программы (операторам, линейным участкам, базисным блокам и т.п.), а дуги — передачам управления между этими операторами. УГП имеет строго одну входную и одну выходную вершину.

Таким образом, будем задавать управляющий граф кортежем  $G = (V, E, s, e, w)$ ,  $s \in V$ ,  $e \in V$ , где  $V \subseteq Insn$  — множество вершин,  $E \in V \times V$  — множество дуг,  $s$  — входная вершина,  $e$  — выходная вершина,  $w$  — отображение, ставящее в соответствие вершинам и дугам графа их вес. Путь  $P$  в графе может быть представлен как упорядоченная последовательность вершин:  $P = (v_1, v_2, \dots, v_i, \dots, v_m)$ ,  $P \in V^*$ . Для каждой вершины и дуги управляющего графа определим вес  $w(v)$ , представляющий собой число прохождений по данной вершине или дуге в ходе тестирования программы:  $w: V \cup E \rightarrow N \cup \{0\}$ . При запуске программы с подачей на вход некоторого тестового



воздействия в управляющем графе проходит некоторый путь (трасса), при этом веса проходимых дуг увеличиваются на 1 при каждом прохождении. Таким образом, на основе данного графа может быть определено значение покрытия ветвей:

$$C_b = \frac{|\{e: e \in E \wedge w(e) > 0\}|}{|E|}.$$

Данное значение будем использовать в качестве критерия полноты тестирования (целью является достижение значения  $C_b = 1$ ).

Управляющий граф программы может быть легко построен по базовой модели программы, поскольку последняя определяет как множество инструкций, так и связи по управлению между ними: в качестве множества вершин графа выбирается множество инструкций всех базисных блоков программы, а множество дуг определяется исходя из связей по управлению между инструкциями.

### Общая схема подхода

В рамках предлагаемого подхода выбор последующих тестовых воздействий будем осуществлять на основе фактических путей и символьных зависимостей переменных, полученных при предыдущих тестовых запусках. С целью получения этих сведений каждый тестовый запуск производится с помощью динамического символьного выполнения, при этом первый тестовый запуск производится с подачей на вход программы произвольного тестового воздействия. При тестировании выполняется следующая последовательность действий:

1) Первый запуск программы осуществляется с подачей на вход тестового воздействия, сгенерированного случайным образом. Входные данные помечаются в исходном тексте тест-драйвера программистом.

2) Перед каждым выполнением программы осуществляется построение алгебраической модели программы и вставка инструментального кода с использованием виртуальной машины Valgrind:

- Valgrind осуществляет декомпиляцию тестируемой программы и ее разбиение на базисные блоки. Каждый блок разбирается с целью определения характера выполняемых в нем инструкций. На основании этих данных осуществляется построение модели программы;
- в каждый блок добавляется инструментальный код отслеживания операций с памятью и пути передачи управления в программе;
- осуществляется компиляция модифицированных базисных блоков в машинный код целевой ЭВМ;
- в переменные, помеченные программистом как входные, записываются значения из текущего тестового воздействия;
- модифицированный код тестируемой программы выполняется центральным процессором ЭВМ непосредственно. При этом добавленный инструментальный код выполняет сбор статистики по тестовому покрытию и осуществляет динамическое символьное выполнение, сохраняя конкретные и символьные значения переменных и условий прохождения ветвлений.

3) После тестового запуска становится известным путь, пройденный в программе, и условие его прохождения в символьном виде. На основании этих данных выбирается следующий тестовый путь и соответствующее ему тестовое воздействие, после чего осуществляется переход к шагу 2. Если достигнуто требуемое значение тестового покрытия, тестирование может быть завершено.

### Символьное выполнение

При каждом тестовом запуске производится динамическое символьное выполнение (рис. 2) от точки входа *entry* до точки выхода *exit*, при котором для каждой переменной  $x$  в памяти сохраняются следующие значения:

- 1) конкретные (численные) значения, определяемые отображением

$$val: Addr \times Types \rightarrow Q,$$

ставящее в соответствие каждой переменной, располагающейся по данному адресу и имеющей заданный тип, ее численное значение (которое будем в дальнейшем называть конкретным значением);

- 2) символьные значения, определяемые отображением

$$sym: Addr \times Types \rightarrow Expr \cup \{\lambda\},$$

ставящее в соответствие каждой переменной, располагающейся по данному адресу и имеющей заданный тип, ее символьное значение;

- 3) входные переменные, определяемые отображением

$$input: Addr \times Types \rightarrow Terms \cup \{\lambda\}.$$

Входные переменные непосредственно доступны для изменения в процессе тестирования.

Сохранение для каждой программной переменной одновременно конкретного и символьного значения позволяет в том числе определять символьные значения целей указательных переменных при их разыменовании.

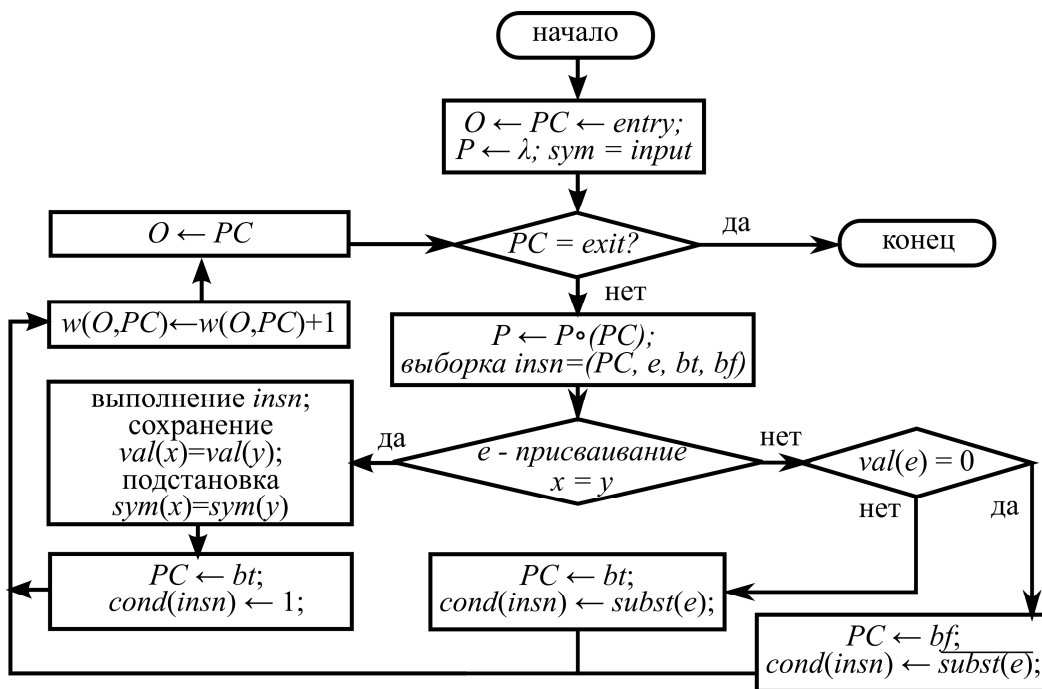


Рис. 3. Алгоритм динамического символьного выполнения

Для удобства введено обозначение пустого кортежа  $\lambda$ , которое будем использовать для записи отсутствия объекта по определенному адресу памяти.

Суть символического выполнения заключается в подстановке в выражение каждой выполняемой инструкции символических значений ее операндов. Подставляя эти значения в условия прохождения ветвлений, получаем необходимые выражения для выбора тестовых воздействий. Результатом является пройденный тестовый путь  $P = (v_0, \dots, v_k)$ , веса дуг управляющего графа  $w(v_i, v_{i+1})$  и условия прохождения вершин управляющего графа  $cond(v_i)$ , принадлежащих тестовому пути. Роль термов в выражениях условий играют константы и входные переменные *input* – таким образом, решая систему условий, получаем соответствующее ей тестовое воздействие.

На рис. 4 наглядно изображено символическое выполнение двух последовательно расположенных машинных инструкций — инструкции присваивания и инструкции ветвления.

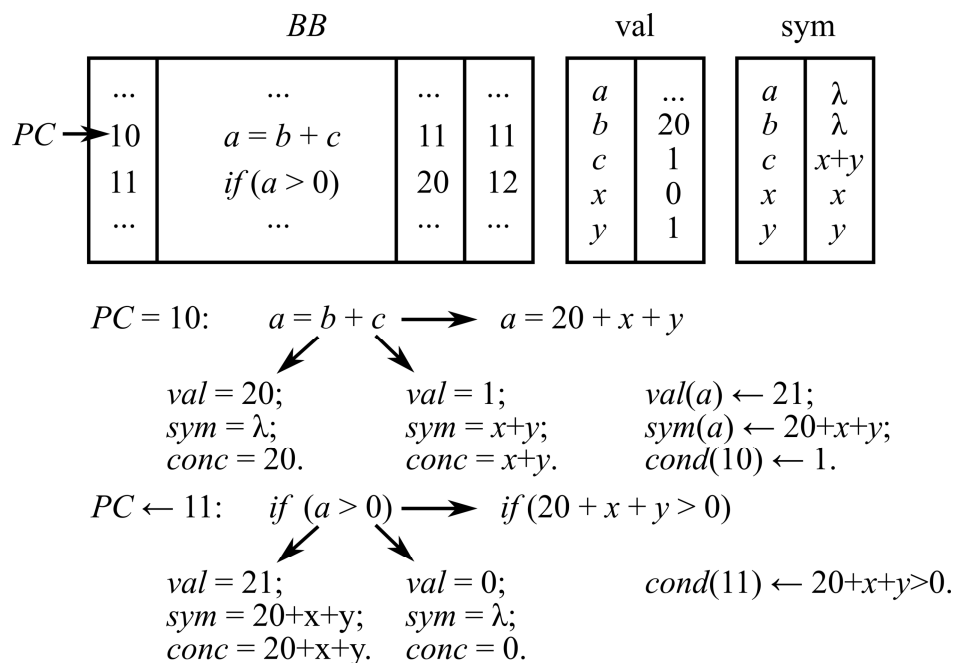


Рис. 4. Пример динамического символического выполнения

### Выбор тестовых путей

По завершении символического выполнения на основе полученных данных о покрытии и условии прохождения текущего пути осуществляется выбор следующего тестового пути. Предположим, что при некотором тестовом запуске был пройден тестовый путь  $P = (v_1, v_2, \dots, v_n)$ , и были определены условия прохождения его вершин  $cond(v_i)$ .

Чтобы определить тестовое воздействие, приводящее к прохождению некоторого альтернативного тестового пути, нам нужно:

- 1) Найти непокрытую дугу  $e = (v_k, v_k^*)$  в управляющем графе, начальная вершина которой  $v_k$  принадлежит пути  $P = (v_0, v_1, \dots, v_i, v_{i+1}, \dots, v_k)$ . Поскольку все дуги рассматриваемого пути были покрыты при предыдущем тестовом запуске,  $v_k^*$  не может принадлежать  $P$  — т.е. дуга  $e$  может начинаться только в инструкции ветвления.

2) Найти нарушающее условие  $c$  в виде конъюнкции условий прохождения вершин пути  $P$  от начальной до  $v_k$  включительно и инверсии условия вершины  $v_{k+1}$ :

$c = \overline{\text{cond}(v_{i+1})} \bigwedge_{j=0}^i \text{cond}(v_j)$ . Инверсия последнего условия требуется, чтобы управление в инструкции ветвления  $v_k$  передавалось по альтернативной дуге  $e$ .

3) Найти тестовое воздействие, решив нарушающее условие.

После каждого тестового запуска просматриваются все пройденные ранее пути на предмет наличия непокрытых дуг, исходящих из принадлежащих им вершин. При отсутствии таких дуг тестирование может быть завершено (поскольку достигнуто полное покрытие ветвей). Блок-схема алгоритма выбора тестовых путей и тестовых воздействий приведена на рис. 5.

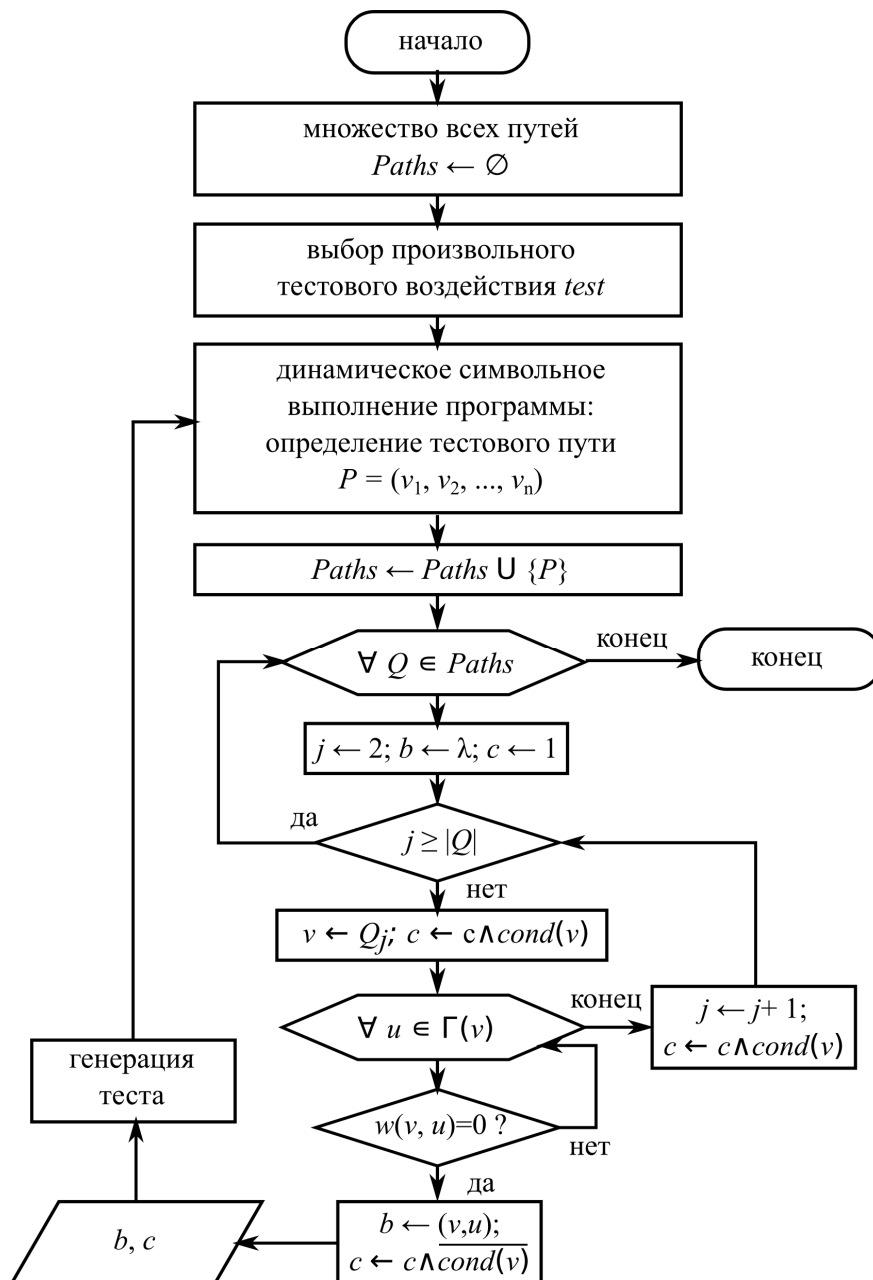


Рис. 5. Алгоритм выбора тестовых путей и тестовых воздействий

Преимуществом представленного подхода по сравнению с существующими является как учет операций над указателями в базовой модели и символьном выполнении, так и анализ программы на уровне машинного кода, позволяющий избежать синтаксического анализа и решить проблему обработки вызовов сторонних подпрограмм.

### Программная реализация

На основе предложенных в настоящей работе моделей и алгоритмов была разработана программная система автоматизации тестирования, предназначенная для тестирования программ, реализованных на компилируемых языках программирования.

Система предоставляет следующие функциональные возможности:

1) Генерация тестовых воздействий на основе динамического символьного выполнения (с целью автоматизации модульного тестирования ПО).

2) Подсчет покрытия кода (покрытие строк и ветвей) без необходимости сборки специальных исполняемых образов.

3) Визуализация покрытия кода в динамике без необходимости перезапуска тестируемой программы.

4) Сохранение дампов трасс выполнения программы с целью отложенного анализа и локализации дефектов.

5) Независимость от используемого языка программирования, поскольку отслеживание выполнения программы производится на уровне отдельных инструкций машинного кода.

6) Поддержка различных аппаратных архитектур ЭВМ. Система поддерживает все архитектуры, для которых реализована трансляция кода в Valgrind (x86, AMD64, POWER, ARM).

Система состоит из трех модулей – инструментального модуля, модуля анализа и тест-драйвера, связанных между собой разделяемой памятью (рис. 6). Инструментальный модуль основан на свободно распространяемой утилите Valgrind, представляющей собой виртуальную машину на основе динамической рекомпиляции. Инструментальный модуль отслеживает адреса и характер выполняемых инструкций и операций с памятью, и отправляет трассу в модуль анализа, вставляя для этого в тестируемую программу необходимый код на этапе выполнения. Задачей модуля анализа является как оценка тестового покрытия кода, так и выбор тестовых путей и определение тестовых воздействий на основе результатов символьного выполнения с последующей передачей найденных значений тест-драйверу.

Данная система использовалась в ходе вычислительных экспериментов, результаты которых приведены ниже.

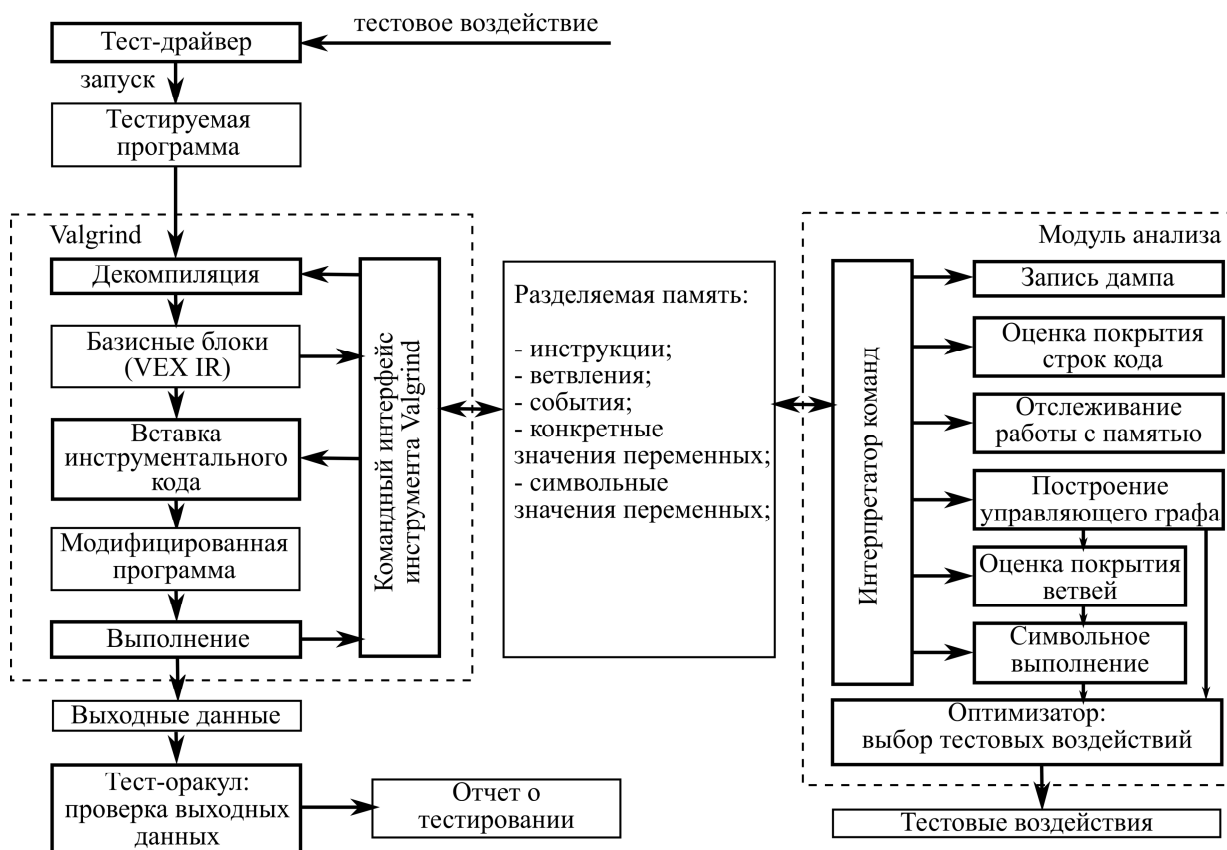


Рис. 6. Архитектура системы

### Эксперимент 1. Модульное тестирование

В ходе экспериментов проводилось сравнение разработанной системы с открытой системой CREST [1], ориентированной на тестирование программ на языке C, и случайным тестированием с использованием следующих тестовых программ:

- сортировка методом выбора главного элемента (*sort*);
- сортировка указателей методом выбора главного элемента (*psort*);
- модифицированные варианты с добавленным ветвлением вида *if(a[i]==13)*;
- вычисление частичной суммы числового ряда (*series*);
- быстрая сортировка, реализованная вручную (*qsort*);
- быстрая сортировка из стандартной библиотеки C (*qsort\_std*) – выполнялось тестирование обратного вызова функции сравнения;
- вставка и последующее удаление элементов в черно-красное дерево (*rbtree*) из реализации *std::set* в GNU libstdc++.

В процессе тестирования определялось достигнутое покрытие ветвей. Результаты (достигнутое покрытие ветвей  $C_b$  и число тестовых воздействий  $N$ , при котором достигнуто указанное покрытие) приведены в таблице 1.

Интерпретация результатов следующая. Примеры *sort* и *psort* оказались достаточно простыми для достижения полного покрытия кода для всех трех методов. В программах *sort\** и *psort\** система CREST не смогла найти добавленное ветвление из-за отсутствия поддержки операций с указателями. В примере *series* достичь полного покрытия удалось только с помощью символического выполнения из-за строгого условия входа в подпрограмму, которое при случайном тестировании никогда не выполнялось, при этом разработанная система достигла полного покрытия ветвей меньшим числом тестов. Аналогичная ситуация наблюдается в примере *qsort* (сложные условия

ветвлений не могут быть проверены полностью случайным тестированием). Примеры `qsort` и `rbtree` система CREST выполнить не смогла, разработанная же в настоящей работе система показывает в целом лучшие результаты, чем случайное тестирование.

**Таблица 1.**

Результаты сравнительных экспериментов

| Тест                   | случайное тестирование |       | CREST |       | разработанная система |       |
|------------------------|------------------------|-------|-------|-------|-----------------------|-------|
|                        | $N$                    | $C_b$ | $N$   | $C_b$ | $N$                   | $C_b$ |
| <code>sort</code>      | 4                      | 1     | 4     | 1     | 4                     | 1     |
| <code>psort</code>     | 4                      | 1     | 4     | 1     | 4                     | 1     |
| <code>sort*</code>     | 4                      | 0,93  | 9     | 0,93  | 4                     | 1     |
| <code>psort*</code>    | 4                      | 0,94  | 9     | 0,94  | 4                     | 1     |
| <code>series</code>    | -                      | 0     | 8     | 1     | 6                     | 1     |
| <code>qsort</code>     | 13                     | 0,94  | 8     | 1     | 5                     | 1     |
| <code>qsort_std</code> | 3                      | 1     | -     | 0     | 3                     | 1     |
| <code>rbtree</code>    | 13                     | 1     | -     | 0     | 6                     | 1     |

## Эксперимент 2. Интеграционное дизайн-тестирование

В качестве эксперимента производилось тестирование одного из компонентов самой системы автоматизации тестирования – граничного решателя, основанного на генетическом алгоритме, а также его графического интерфейса пользователя. Компонент написан на C++/Qt4, состоит из примерно 20 тысяч строк исходного текста (с учетом транслятора символьных условий, базовых библиотек и графического интерфейса), графический интерфейс предоставляет следующую функциональность:

- ввод и компиляцию в машинный код целевой функции в виде алгебраического выражения;
- минимизацию значения целевой функции с помощью генетического алгоритма с использованием распараллеливания;
- визуализацию результатов оптимизации и графиков изменения целевой функции в зависимости от итерации.

Тестирование производилось в интерактивном режиме, в качестве объекта тестирования было выбрано множество классов элементов пользовательского интерфейса, отвечающих за ввод и вывод данных. В процессе тестирования система в динамике обновляет тестовое покрытие по подпрограммам и методам классов и выдает подсказки по выбору тестов.

При тестировании было использовано 24 тестовых воздействия, 10 дуг управляющего графа были помечены как нереализуемые (ветви обработки ошибок в операторах ASSERT, не воспроизводящиеся на практике). С учетом них было достигнуто полное покрытие ветвей тестируемых участков кода.

## Эксперимент 3. Тестирование производительности

Немаловажным фактором, ограничивающим применимость той или иной системы динамического анализа программ, является влияние инструментирования на временные соотношения работы программы. Под производительностью далее будем понимать производительность среды исполнения программы (аппаратного обеспечения и виртуальной машины) в виде количества машинных инструкций, исполняемых в

среднем в единицу времени. Очевидно, что определенная таким образом производительность зависит от характера выполняемых инструкций, поэтому можно использовать ее только с целью сравнения различных сред исполнения при выполнении одной и той же программы. В табл. 2 приведены результаты синтетического теста Dhystone [4], выполненного с использованием различных вариантов инструментирования.

Результаты синтетического теста наглядно показывают превосходство в плане производительности инструментирования на уровне исходных текстов (GCC/gcov). Динамическая рекомпиляция в Valgrind приводит к падению производительности в 4-5 раз даже без вставки инструментального кода — данные накладные расходы являются платой за гибкость динамических методов инструментирования. Для сравнения приведена производительность, достигнутая встроенным инструментом Valgrind memcheck.

Наибольшее влияние на производительность оказывает отслеживание операций с памятью. По сравнению с накладными расходами от этого инструментального кода влияние символьного выполнения практически не заметно. Оптимальная расстановка точек инструментирования здесь представляет собой несомненно важную и интересную задачу и является одним из направлений дальнейшего исследования.

Таблица 1.

Результаты синтетического теста

| Тип запуска                              | Производительность, DMIPS | Время выполнения одной итерации, мкс |
|--|---------------------------|--------------------------------------|
| Без инструментирования                   | 6587                      | 0.09                                 |
| GCC/gcov                                 | 5591                      | 0.10                                 |
| Valgrind (только рекомпиляция)           | 1504                      | 0.39                                 |
| Valgrind (memcheck)                      | 166                       | 3.43                                 |
| Покрытие ветвей                          | 544                       | 1.05                                 |
| Запись дампа                             | 547,2                     | 1.04                                 |
| Отслеживание памяти (помеченные участки) | 45,5                      | 12.6                                 |
| Отслеживание памяти (все операции)       | 11,8                      | 48.0                                 |
| Динамическое символьное выполнение       | 11,7                      | 48.6                                 |

Полученные результаты естественным образом ограничивают применимость представленного подхода модульным тестированием, при котором производительность обычно не является критичной. С другой стороны, оценка покрытий в динамике без отслеживания операций с памятью полезна при выполнении ручного дизайн-тестирования сложной программной системы.

## Выводы

Результаты вычислительных экспериментов показывают, что предложенный метод модульного тестирования в ряде случаев позволяет достичь большего тестового покрытия по сравнению с известными методами. Достигается данный результат в основном за счет динамического анализа программ на уровне машинных кодов и отслеживания операций с указателями. Разработанная авторами программная система с



успехом может применяться как для автоматизации модульного тестирования, так и для облегчения ручного тестирования (в частности, интеграционного тестирования) программных систем на этапе разработки. С другой стороны, динамический анализ программ оказывает сильное влияние на производительность, что ограничивает сферу его применения, в частности, делая символьное выполнение неприменимым на практике для тестирования программной системы в целом. Тем не менее, приведенные в данном разделе проблемы являются техническими и поддаются решению. Таким образом, настоящая работа имеет большой потенциал для дальнейшего исследования – в частности, могут быть сформулированы следующие задачи:

- задача оптимальной расстановки точек инструментирования;
- задача обнаружения и удаления ненужного инструментального кода;
- задача неинтрузивного вычисления тестового покрытия кода.

Решение данных задач в перспективе позволит применять предложенные методы с целью проведения тестирования безопасности и обнаружения уязвимостей в программных системах на уровне интеграционного и системного тестирования.

### Список литературы

1. Burnim, J. Heuristics for Scalable Dynamic Test Generation / J. Burnim, K. Sen // Proceedings of the 23<sup>rd</sup> IEEE/ACM International Conference on Automated Software Engineering. — IEEE Computer Society Press, 2008. — PP. 443–446.
2. Nethercote, N. Valgrind: a Framework for Heavyweight Dynamic Binary Instrumentation / N. Nethercote, J. Seward // Proceedings of the 2007 ACM SIGPLAN Conference on Programming Language Design and Implementation. — ACM, New York, 2007. — PP. 89–100.
3. Ломакина, Л.С. Модели и методы тестирования программных систем на основе алгебраического подхода / Л.С. Ломакина, А.Н. Вигура // Системы управления и информационные технологии. — Воронеж, 2013. — Том 52, № 2.1. — С. 157–161.
4. Weicker, R.P. Dhrystone: a synthetic systems programming benchmark / R.P. Weicker // Communications of the ACM. — 1984. — Vol. 27, Iss. 10. — PP. 1013–1030.

**СТРУКТУРНЕ ТЕСТУВАННЯ ПРОГРАМНИХ СИСТЕМ З ВИКОРИСТАННЯМ ЕЛЕМЕНТІВ  
КОМП'ЮТЕРНОЇ АЛГЕБРИ**

Л.С. Ломакіна, А.М. Вігура

Нижегородський державний технічний університет ім. Р.С. Алексєєв,  
вул. Мініна, 24, Нижній Новгород, 603950, Російська Федерація; e-mail: llomakina@list.ru

Запропоновано метод структурного тестування програмних систем, заснований на алгебраїчній моделі програми і динамічному символічному виконанні на рівні машинного коду і дозволяє автоматизувати модульне тестування програм, реалізованих на компільованих мовах програмування.

**Ключові слова:** програмні системи, тестування, генерація тестових даних, алгебраїчна модель, символічне виконання

**STRUCTURAL TESTING OF SOFTWARE SYSTEMS USING ELEMENTS OF COMPUTER  
ALGEBRA**

Lyubov S. Lomakina, Anton N. Vigura

Nizhny Novgorod State Technical University n.a. R.E. Alekseev,  
24 Minina str., Nizhny Novgorod, 603950, Russian Federation; llomakina@list.ru

A method of software system structural testing based on the program algebraic model and machine code-level dynamic symbolic execution is proposed. The method allows for unit testing automation for programs written in compiled languages.

**Keywords:** software systems, testing, test data generation, algebraic model, symbolic execution

# ОПРЕДЕЛЕНИЕ ОПТИМАЛЬНЫХ ПАРАМЕТРОВ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ ПО СОСТОЯНИЮ СЛОЖНЫХ ОБЪЕКТОВ РАДИОЭЛЕКТРОННОЙ ТЕХНИКИ

С.В. Ленков<sup>1</sup>, А.В. Селюков<sup>2</sup>, В.В. Зубарев<sup>3</sup>, В.Н. Цыцарев<sup>1</sup>

<sup>1</sup> Военный институт Киевского национального университета имени Тараса Шевченко,  
ул. Ломоносова, 81, Киев, 03680, Украина; e-mail: lenkov\_s@ukr.net

<sup>2</sup> Государственное предприятие «Научный центр точного машиностроения»,  
ул. Бориспольская, 9, Киев, 02099, Украина; e-mail: selukov@3g.ua

<sup>3</sup> Центральный научно-исследовательский институт вооружения и военной техники ВС Украины,  
Киев, Украина

Предложены методика и алгоритм решения задачи определения оптимальных параметров технического обслуживания по состоянию сложных объектов радиоэлектронной техники. Задача оптимизации ставится как задача минимизации удельной стоимости эксплуатации объекта при заданном ограничении на минимально допустимый уровень безотказности объекта.

В качестве оптимизируемых параметров процесса технического обслуживания по состоянию приняты: 1) множество обслуживаемых элементов объекта, 2) уровни предельно допустимых значений определяющих параметров обслуживаемых элементов, и 3) периодичность контроля технического состояния объекта.

Целевые функции задачи – удельная стоимость эксплуатации и средняя наработка на отказ объекта получаются с помощью имитационной статистической модели. Задача решается приближенно с использованием разработанного программного обеспечения. В поиске оптимального решения принимает участие в интерактивном режиме человек-эксперт. Приводится пример решения задачи.

**Ключевые слова:** техническое обслуживание, радиоэлектронная техника, эксплуатация

## Введение

Техническое обслуживание (ТО) для сложных объектов радиоэлектронной техники (РЭТ) является одним из средств обеспечения требуемого уровня надежности объектов в процессе эксплуатации. Если требуемый уровень надежности обеспечивается и без всякого ТО, то вопрос о необходимости ТО вообще снимается. Однако для многих типов сложных объектов РЭТ проблема обеспечения их надежности все же остается актуальной, несмотря на применение современной элементной базы и новых технологий разработки и изготовления аппаратуры. Для таких объектов разработчик всегда стремится использовать все возможные меры для повышения надежности, в том числе и ТО. В этих случаях разработчику важно знать, какая потенциально возможная прибавка в уровне надежности объекта может быть получена за счет ТО и какие дополнительные стоимостные затраты для этого могут потребоваться.

Задача состоит в следующем: для заданного типа объекта РЭТ с известными составом, структурой, надежностными и стоимостными характеристиками требуется

определить оптимальные параметры системы ТО (СТО). Оптимальные параметры СТО должны обеспечивать заданный уровень надежности объекта при минимальных затратах на его эксплуатацию. Задачу будем решать для стратегии ТО «по состоянию» (ТОС), которая считается потенциально наиболее эффективной. Однако для практической реализации стратегии ТОС конструкция объекта должна быть приспособлена для этого, в частности, необходимо, чтобы для обслуживаемых элементов существовали измеряемые определяющие параметры (ОП).

Процесс ТО, организованный в соответствии со стратегией ТОС, должен протекать следующим образом. В процессе эксплуатации производится периодический контроль технического состояния (ТС) обслуживаемых элементов. Если в результате контроля оказывается, что ТС элемента не соответствует требуемому, выполняется ТО (или замена) этого элемента.

Обозначим  $E_{\text{то}} = \{e_i\}$  множество обслуживаемых элементов объекта, и будем полагать, что для всех обслуживаемых элементов существуют ОП. Нормированное значение ОП, измеренное в момент времени  $t$ , будем обозначать  $u_i(t)$ . Величина  $u_i(t)$  может принимать значения в диапазоне  $[0,1]$ , значение  $u_i(t) = 0$  соответствует номинальному значению ОП, значение  $u_i(t) = 1$  является критическим, при достижении которого наступает отказ элемента. Для каждого элемента  $e_i \in E_{\text{то}}$  задается уровень ТО  $u_{\text{то}i}$  такой, что если при контроле оказывается, что  $u_i(t) \geq u_{\text{то}i}$ , то производится замена элемента  $e_i$ .

С учетом введенных обозначений и понятий постановку задачи оптимизации параметров ТОС запишем формально следующим образом [1]:

$$\begin{aligned} T_0(E_{\text{то}}^*, U_{\text{то}}^*, T_k^*) &\geq T_0^{\text{тп}}, \\ c_0(E_{\text{то}}^*, U_{\text{то}}^*, T_k^*) &\rightarrow \min, \end{aligned} \quad (1)$$

где

$T_0^{\text{тп}}$  — заданное требуемое значение средней наработки на отказ объекта;

$E_{\text{то}}^*$ ,  $U_{\text{то}}^*$  и  $T_k^*$  — искомые оптимальные значения параметров ТОС:  $E_{\text{то}}$  — множество обслуживаемых элементов;  $U_{\text{то}} = \{u_{\text{то}i}; i = \overline{1, |E_{\text{то}}|}\}$  — вектор уровней ТО  $u_{\text{то}i}$ ;  $T_k$  — периодичность контроля объекта.

Сложность решения данной задачи обусловлена двумя обстоятельствами. Во-первых – это сложная структура пространства, в котором должен осуществляться поиск оптимальных значений  $E_{\text{то}}^*$ ,  $U_{\text{то}}^*$  и  $T_k^*$ . Пространство это представляет собой декартово произведение

$$\{E_{\text{то}}\} \times [0,1]^{|E_{\text{то}}|} \times [0, \infty), \quad (2)$$

где

$\{E_{\text{то}}\}$  — множество всех множеств  $E_{\text{то}}$ , где  $E_{\text{то}}$  — множество потенциально обслуживаемых элементов ( $E_{\text{то}}^* \subseteq E_{\text{то}}$ );

$[0,1]^{|E_{\text{то}}|}$  — гиперкуб, каждая точка в котором представляет собой вектор размерностью  $|E_{\text{то}}|$ , элементами вектора являются числа, принадлежащие отрезку  $[0,1]$ ;

$[0, \infty)$  — числовая ось, содержащая все положительные числа.

Во-вторых, особенностью задачи (1), осложняющей ее решение, является то, что для ее целевых функций  $T_0$  и  $c_3$  неизвестны аналитические выражения, их значения в отдельных точках могут быть получены только путем моделирования [2]. С учетом этого очевидно, что можно рассчитывать, по всей видимости, только на приближенное решение задачи (1).

В данной статье предлагается методика приближенного решения задачи (1), представленная описываемым ниже алгоритмом. Алгоритм основан на применении имитационной статистической модели (ИСМ) [2].

### Алгоритм решения задачи

Структурная схема алгоритма решения задачи (1), приведена на рис. 1. Исходной информацией для алгоритма являются вся информация об объекте РЭТ, которая используется ИСМ [2], дополнительно также задаются множество потенциально обслуживаемых элементов  $E_{\text{ТО}}$  и требуемое значение средней наработки на отказ объекта  $T_0^{\text{ТР}}$ .

Оператор 1 создает множества  $E_{\text{ТО}i}^+$  и  $U_{\text{ТО}i}^+$  (вначале пустые), и иницирует переменную  $i$ , которая используется для подсчета числа выполненных шагов поиска решения (одновременно переменная  $i$  является номером элемента  $e_i$ , который добавлен в множество  $E_{\text{ТО}i}^+$  последним). Множество  $E_{\text{ТО}i}^+$  используется в качестве текущего множества обслуживаемых элементов (в него на каждом шаге будет добавляться один элемент, взятый из множества  $E_{\text{ТО}}$ ). Множество (вектор)  $U_{\text{ТО}i}^+$  используется для запоминания найденных оптимальных значений уровней ТО  $u_{\text{ТО}i}^+$  элементов, уже включенных в множество  $E_{\text{ТО}i}^+$ .

Оператор 2 формирует номер  $i$  очередного (текущего) шага процесса поиска.

Оператор 3 выбирает из множества  $E_{\text{ТО}}$   $i$ -й элемент  $e_i$  и добавляет его в множество  $E_{\text{ТО}i}^+$ . Выбор элементов  $e_i$  из  $E_{\text{ТО}}$  производится в порядке возрастания их средней наработки до отказа.

Оператор 4 строит (программно) графики функций  $u_{\text{ТО}i}^+(T_k)$  и  $c_3^+(T_k)$  в зависимости от периодичности ТО  $T_k$ .  $u_{\text{ТО}i}^+(T_k)$  — это оптимальное значение уровня ТО для  $i$ -го элемента, найденное из условия:

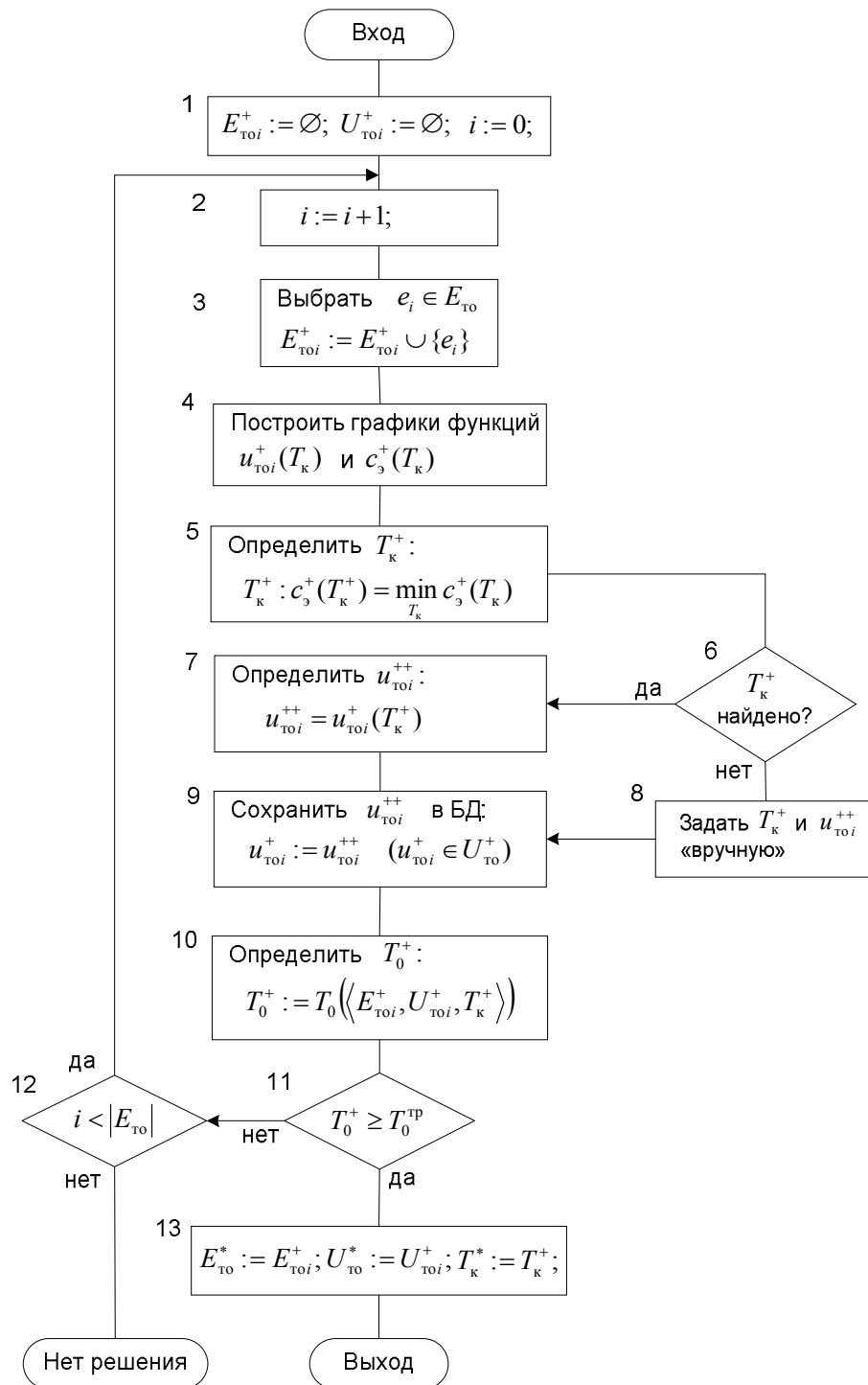
$$u_{\text{ТО}i}^+(T_k): c_3(E_{\text{ТО}i}^+, U_{\text{ТО}i}^+, T_k) \rightarrow \min_{u_{\text{ТО}i} \in U_{\text{ТО}i}^+}, \quad (3)$$

где  $U_{\text{ТО}i}^+ = \{u_{\text{ТО}1}^*, \dots, u_{\text{ТО}i-1}^*, u_{\text{ТО}i}^*\}$  — это вектор, в котором  $u_{\text{ТО}1}^*, \dots, u_{\text{ТО}i-1}^*$  — оптимальные значения уровней ТО элементов  $e_1, \dots, e_{i-1}$ , найденные в предыдущих шагах, а  $u_{\text{ТО}i}$  — варьируемый уровень ТО для элемента  $e_i$ , оптимальное значение которого должно быть найдено в соответствии с условием (3).

Величина  $c_3^+(T_k)$  — это удельная стоимость эксплуатации, получаемая при оптимальном значении уровня ТО  $u_{\text{ТО}i}^+(T_k)$ :

$$c_3^+(T_k) = c_3(E_{\text{ТО}i}^+, U_{\text{ТО}i}^+, T_k). \quad (4)$$

Вектор  $U_{\text{то}}^+$  в (4) отличается от  $U_{\text{то}i}^*$  только тем, что в  $U_{\text{то}}^+$  в качестве  $i$ -ой компоненты подставлено найденное условно оптимальное значение  $u_{\text{то}i}^+(T_k)$ .



**Рис. 1.** Алгоритм поиска оптимальных параметров стратегии ТОС

Оператор 5 определяет оптимальное в текущем шаге (условно оптимальное) значение периодичности контроля  $T_k^+$ , удовлетворяющее условию:

$$c_3^+(T_k^+) = \min_{T_k} c_3^+(T_k). \quad (5)$$

Если величина  $T_k^+$  найдена, то далее выполняется оператор 7, который определяет оптимальное значение уровня ТО  $u_{toi}^{++}$ :

$$u_{toi}^{++} = u_{toi}^+(T_k^+) \quad (6)$$

(здесь «++» подчеркивает тот факт, что значение  $u_{toi}^{++}$  относится к найденному оптимальному значению  $T_k^+$ ).

Оператор 9 найденное значение  $u_{toi}^{++}$  сохраняет в БД в качестве оптимального значения, и тем самым подготавливает БД к расчетам в последующих шагах.

На данной стадии расчетов мы получаем условно оптимальное решение задачи:

$$\langle E_{toi}^+, U_{toi}^+, T_k^+ \rangle.$$

В некоторых случаях минимум у функции  $c_3^+(T_k)$  может отсутствовать. В этих случаях в процесс вмешивается эксперт, который по графикам  $c_3^+(T_k)$  и  $T_0^+(T_k)$  выбирает приемлемое значение  $T_k^+$  и соответствующее ему значение  $T_0^+(T_k^+)$ . Величина  $u_{toi}^{++}$ , соответствующая выбранному  $T_k^+$ , определяется по графику  $u_{toi}^+(T_k)$ . Эти действия эксперта на схеме алгоритма представлены операторами 6 и 8.

Оператор 10 определяет достигнутое в  $i$ -м шаге поиска значение средней наработки на отказ объекта  $T_0^+$ :

$$T_0^+ = T_0(\langle E_{toi}^+, U_{toi}^+, T_k^+ \rangle).$$

Оператор 11 проверяет выполнение условия  $T_0^+ \geq T_0^{TP}$ . Если это условие выполняется, то полученное условно оптимальное решение  $\langle E_{toi}^+, U_{toi}^+, T_k^+ \rangle$  принимается в качестве окончательного решения задачи (оператор 13). Процесс поиска решения в этом случае завершается.

В противном случае, если  $T_0^+ < T_0^{TP}$ , выполняется оператор 12, который проверяет, все ли элементы из  $E_{то}$  были использованы при поиске решения. Если нет ( $i < |E_{то}|$ ), то оператор 12 передает управление оператору 2 для продолжения процесса поиска решения.

Если на некотором шаге все элементы, выбираемые из  $E_{то}$ , будут исчерпаны ( $i = |E_{то}|$ ), то это будет означать, что исходная задача (1) не имеет решения – заданное требование  $T_0^{TP}$  за счет ТО не может быть обеспечено. Полученное на последнем шаге значение средней наработки на отказ  $T_0^+$  – это, по-видимому, максимальное ее значение, которое может быть достигнуто за счет проведения ТОС.

Данный алгоритм реализован программно в рамках программы ISMPN [2]: в программе для этого введен дополнительно режим **Оптимизация ТО | ТО “по состоянию”**.

Для примера воспользуемся тестовым объектом, который мы уже использовали в [2]. Конструктивная структура объекта показана на рис. 2. Составные элементы на рисунке изображены прямоугольниками, простые – кружками. Рядом со значками простых элементов цифрой показано количество однотипных комплектующих элементов (КЕ), входящих в данный элемент. Все простые элементы состоят из одинаковых КЕ, с характеристиками надежности: средняя наработка до отказа  $T_{cp} = 20000$  ч; коэффициент вариации  $\nu = 0.8$ ;  $DN$ -распределение наработки до отказа [3].

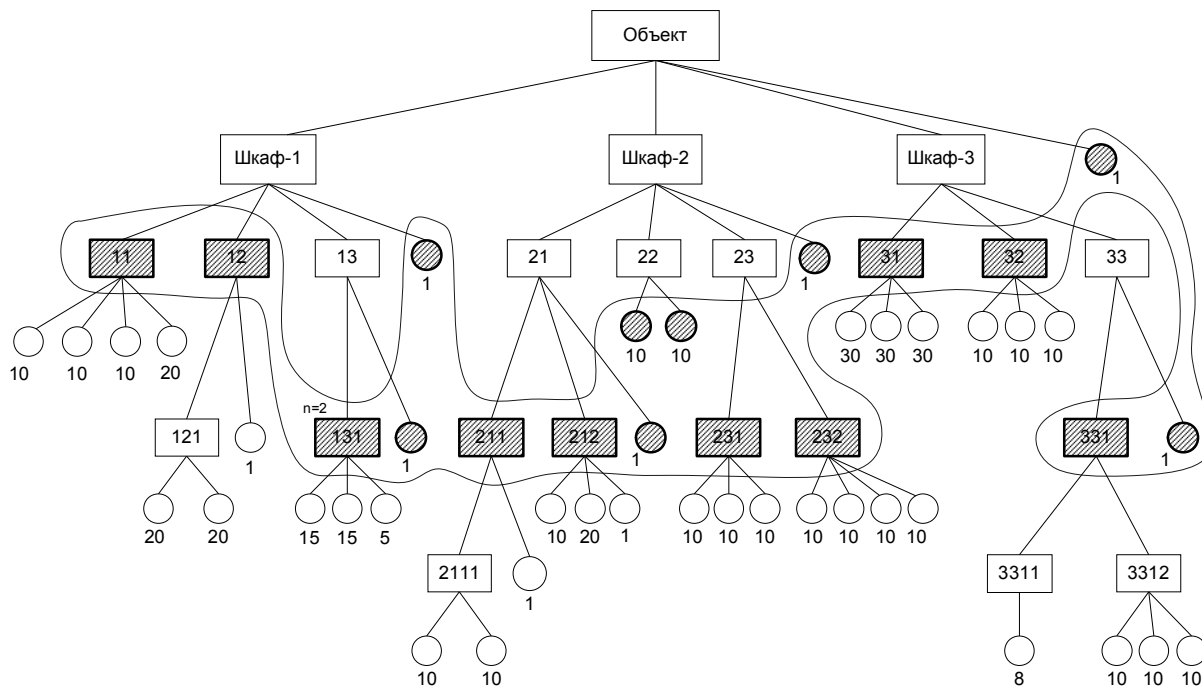


Рис. 2. Конструктивная структура тестового объекта

Подмножество отказывающихся элементов  $E_0$  отмечено на рисунке штриховкой. В множество потенциально обслуживаемых элементов  $E_{то}$  включим 5 наименее надежных элементов из  $E_0$ . Данные об элементах  $E_{то}$  представлены в табл. 1.

Таблица 1.

Характеристики потенциально обслуживаемых элементов тестового объекта

| Номер элемента | Наименование элемента | Средняя наработка до отказа $T_{срi}$ , ч | Стоимость элемента $C_{0i}$ , у.е. |
|----------------|-----------------------|---|------------------------------------|
| 1              | 31                    | 2108                                      | 900                                |
| 2              | 331                   | 2425                                      | 680                                |
| 3              | 11                    | 2828                                      | 500                                |
| 4              | 12                    | 3123                                      | 410                                |
| 5              | 131                   | 3380                                      | 350                                |

Моделирование будем производить на интервале эксплуатации  $T_s = 20$  лет. В результате моделирования для случая, если ТО не проводится, были получены следующие значения показателей:



$$T_0 = 277 \text{ ч}, \quad c_3 = 1.468 \text{ у.е./ч}, \quad K_{\text{ти}} = K_{\Gamma} = 0.99278.$$

Зададим требуемое значение средней наработки на отказ  $T_0^{\text{TP}} = 400 \text{ ч}$ .

В соответствии с приведенным алгоритмом расчеты произведем в следующей последовательности:

На 1-м шаге (в 1-м цикле исполнения алгоритма рис. 1) в множество  $E_{\text{то}}^+$  включим элемент 31:  $E_{\text{то1}}^+ = \{31\}$ .

Запустим программу ISMPN в режиме **Оптимизация ТО | ТО “по состоянию”**. Для поиска условно оптимальных значений  $u_{\text{тоi}}^+$  и  $T_{\text{к}}^+$  зададим следующие интервалы варьирования параметров:

- для  $u_{\text{то}}^+$ : от 0,4 до 0,8 с интервалом 0,05;
- для  $T_{\text{к}}^+$ : от 100 до 500 ч с интервалом 20 ч.

После завершения моделирования вид экрана ПК будет примерно таким, как это показано на рис. 3.

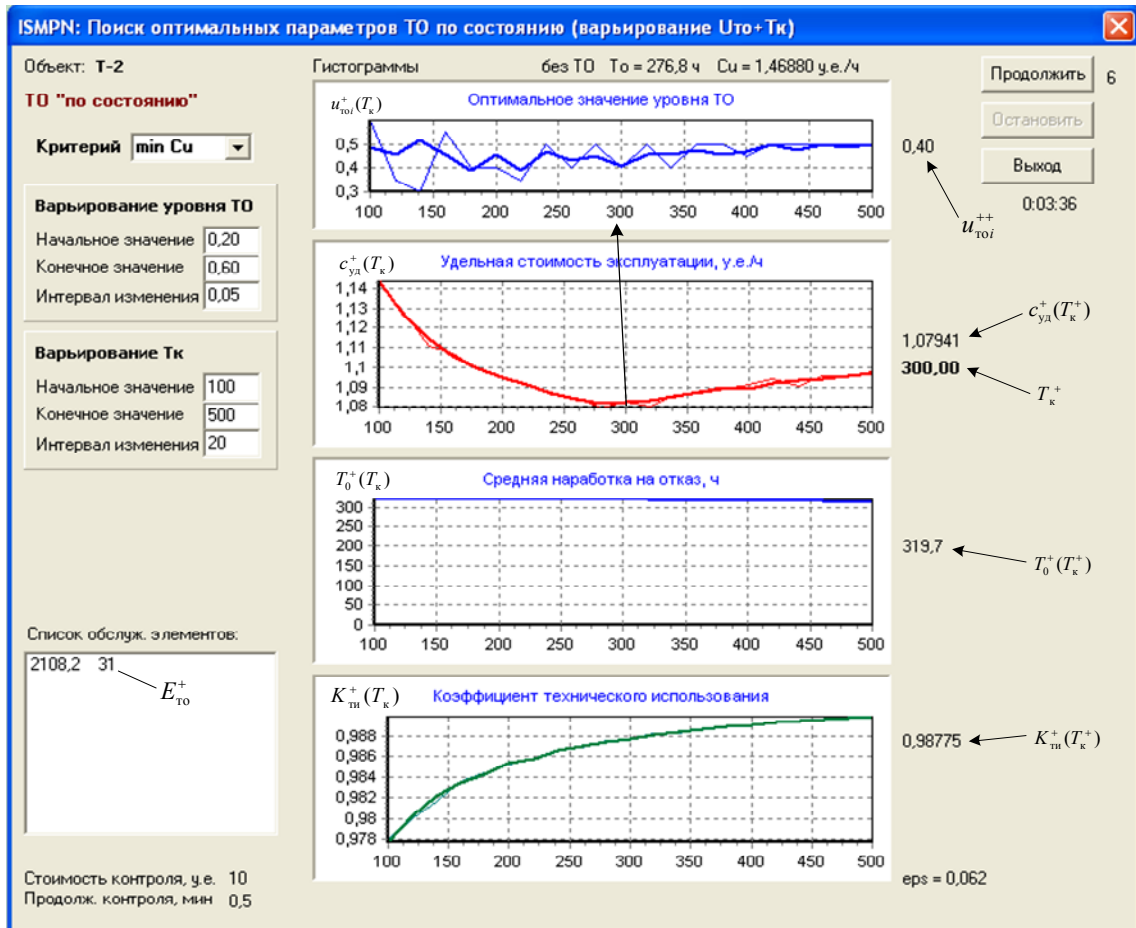


Рис. 3. Вид экрана ПК после завершения расчетов на 1-м шаге

По графику функции  $c_3^+(T_{\text{к}})$  определяем ее минимальное значение  $c_3^+(T_{\text{к}}) = 1.07941$  и соответствующее ему оптимальное значение  $T_{\text{к}}^+ = 300 \text{ ч}$ . По графику  $u_{\text{тоi}}^+(T_{\text{к}})$  определяем оптимальное значение  $u_{\text{то1}}^+ = u_{\text{тоi}}^+(T_{\text{к}}^+) = 0.45$ . Таким образом, в

результате выполнения расчетов на 1-м шаге получаем следующее условно оптимальное решение:

$$\langle E_{\text{то1}}^+, U_{\text{то1}}^+, T_{\text{к}}^+ \rangle = \langle \{31\}, \{0,45\}, 300 \text{ ч} \rangle.$$

По графику  $T_0^+(T_{\text{к}})$  определяем достигнутое значение средней наработки на отказ  $T_0^+ = 319$  ч. Сравнивая полученное значение  $T_0^+ = 319$  ч с требуемым значением  $T_0^{\text{тп}} = 400$  ч, приходим к выводу, что заданное требование не выполняется. Значит необходимо продолжить расчеты и перейти к выполнению следующего шага. Но перед этим необходимо открыть БД и для элемента 31 ввести полученное для него условно оптимальное значение уровня ТО  $u_{\text{то1}}^{++}$ .

Аналогичным образом произведем расчеты на всех последующих шагах, последовательно включая в множество  $E_{\text{то}(i)}^+$  все элементы из  $E_{\text{то}}$  (всего 5 шагов). Для экономии места не будем приводить все промежуточные результаты. Приведем только окончательные данные условно оптимальных решений, полученных на каждом шаге. Данные сведены в табл. 2.

**Таблица 2.**

Результаты расчетов условно оптимальных параметров ТОС для тестового объекта

| Номер шага<br>$i$ | Условно оптимальные параметры<br>$\langle E_{\text{то}i}^+, U_{\text{то}i}^+, T_{\text{к}}^+ \rangle$ |                       |                             | Значения показателей, получаемые при условно оптимальных параметрах |                         |                   |               |
|-------------------|---|-----------------------|-----------------------------|---|-------------------------|-------------------|---------------|
|                   | $E_{\text{то}i}^+$  | $u_{\text{то}i}^{++}$ | $T_{\text{к}}^+, \text{ ч}$ | $T_0^+, \text{ ч}$  | $c_3^+, \text{ у.е./ч}$ | $K_{\text{ти}}^+$ | $\varepsilon$ |
| 0                 | –   | –                     | –                           | 277   | 1,46880                 | 0,99278           | 0,060         |
| 1                 | {31}  | 0,40                  | 300                         | 319   | 1,07941                 | 0,98775           | 0,062         |
| 2                 | {31,331}  | 0,45                  | 280                         | 366   | 0,80331                 | 0,98755           | 0,075         |
| 3                 | {31,331,11}   | 0,42                  | 260                         | 422   | 0,63401                 | 0,98725           | 0,072         |
| 4                 | {31,331,11,12}  | 0,50                  | 280                         | 483   | 0,50673                 | 0,98784           | 0,083         |
| 5                 | {31,331,11,12,131}  | 0,50                  | 280                         | 568   | 0,40421                 | 0,98789           | 0,081         |

По полученным данным видно, что требование  $T_0^{\text{тп}} = 400$  ч выполняется уже на 3-м шаге, с учетом этого в рассматриваемом примере получаем следующее решение задачи (1):

$$\langle E_{\text{то}}^*, U_{\text{то}}^*, T_{\text{к}}^* \rangle = \langle \{31, 331, 11\}; \{0.40; 0.45; 0.42\}, 260 \text{ ч} \rangle.$$

При полученных оптимальных параметрах ТОС будут обеспечиваться следующие значения показателей:

$$T_0 = 422 \text{ ч}, \quad c_3 = 0.63401 \text{ у.е./ч}, \quad K_{\text{ти}} = 0.98725.$$

Статистическая ошибка результатов моделирования (относительная ошибка оценки  $T_0$ ), при которой получены эти результаты, равна  $\varepsilon = 0.072$ .

## Выводы

1) Рассмотренные алгоритм и методика позволяют решать поставленную задачу определения оптимальных параметров ТОС с приемлемой для практики точностью.

2) Разработанное программное обеспечение для решения данной задачи может применяться при разработке объектов РЭТ в качестве адекватного инструмента для прогнозирования показателей их эксплуатационной надежности с учетом проведения ТОС.

3) Получаемые прогнозные оценки показателей  $T_0$ ,  $c_3$  и  $K_{ти}$  являются оптимистическими (завышенными) вследствие того, что алгоритм моделирования основан на допущении о существовании и возможности измерения ОП для всех обслуживаемых элементов объекта. На практике такое допущение, к сожалению, далеко не всегда можно реализовать.

## Список литературы

1. Моделирование и оптимизация процессов технического обслуживания сложных объектов радиоэлектронной техники: Монография / Ю.В. Березовская, К.Ф. Боряк, В.О. Браун, С.В. Ленков, В.А. Осыпа, С.А. Пашков, В.Н. Цыцарев и др.; под ред. С.В. Ленкова. — 1-е издание. — Николаев: Сент-Гросс, 2012. — 150 с.
2. Ленков, С.В. Прогнозирование показателей надежности и стоимости эксплуатации сложных объектов РЭТ с использованием имитационной статистической модели / С.В. Ленков, В.О. Браун, В.А. Осыпа и др. // Збірник наукових праць Військового інституту Київського національного університету ім. Тараса Шевченка. — К., 2013. — № 43. — С. 22–25.
3. ГОСТ 27.005-97. Надежность в технике. Модели отказов. Основные положения. — Введ. 01.01.99. — 45 с.

## ВИЗНАЧЕННЯ ОПТИМАЛЬНИХ ПАРАМЕТРІВ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ ЗА СТАНОМ СКЛАДНИХ ОБ'ЄКТІВ РАДІОЕЛЕКТРОННОЇ ТЕХНІКИ

С.В. Ленков<sup>1</sup>, О.В. Селюков<sup>2</sup>, В.В. Зубарев<sup>3</sup>, В.М. Цыцарев<sup>1</sup>

<sup>1</sup> Військовий інститут Київського національного університету імені Тараса Шевченка, вул. Ломоносова, 81, Київ, 03680, Україна; e-mail: lenkov\_s@ukr.net

<sup>2</sup> Державне підприємство «Науковий центр точного машинобудування», вул. Бориспільська, 9, Київ, 02099, Україна; e-mail: selukov@3g.ua

<sup>3</sup> Центральний науково-дослідний інститут озброєння і військової техніки ЗС України, Київ, Україна

Запропоновано методику та алгоритм розв'язання задачі визначення оптимальних параметрів технічного обслуговування за станом складних об'єктів радіоелектронної техніки. Завдання оптимізації розглядається як завдання мінімізації питомої вартості експлуатації об'єкта при заданому обмеженні на мінімально допустимий рівень безвідмовності об'єкта.

В якості оптимальних параметрів процесу технічного обслуговування за станом прийняті: 1) безліч обслуговуваних елементів об'єкта, 2) рівні гранично допустимих значень визначальних параметрів обслуговуваних елементів, та 3) періодичність контролю технічного стану об'єкта.

Цільові функції завдання – питома вартість експлуатації та середнє напрацювання на відмову об'єкта виходять за допомогою імітаційної статистичної моделі. Задача вирішується з використанням розробленого програмного забезпечення. У пошуку оптимального рішення приймає участь в інтерактивному режимі людина-експерт. Наводиться приклад розв'язання задачі.

**Ключові слова:** технічне обслуговування, радіоелектронна техніка, експлуатація

## DETERMINATION OF THE OPTIMAL PARAMETERS OF MAINTENANCE AS FOR THE CONDITION OF COMPOUND FACILITIES OF RADIO ELECTRONIC EQUIPMENT

Sergey V. Lenkov<sup>1</sup>, Oleksandr V. Selyukov<sup>2</sup>, Valery V. Zubarev<sup>3</sup>, Vadim M. Tsytsaryev<sup>1</sup>

<sup>1</sup> Military Institute, Taras Shevchenko National University of Kyiv, 81 Lomonosov str., Kyiv, 03680, Ukraine; e-mail: lenkov\_s@ukr.net

<sup>2</sup> Scientific center of precision engineering, State enterprise, 9 Boryspilska str., Kyiv, 02099, Ukraine; e-mail: selukov@3g.ua

<sup>3</sup> Central Research Institute of weapons and military equipment, Kyiv, Ukraine

The methods and algorithm for problem solving concerning the determination of the optimal parameters of maintenance as for the condition of compound facilities of radio electronic equipment were proposed. The optimization problem is set as a problem of minimizing the cost factor of the facility maintenance given the restriction to minimum permissible level of the facility reliability.

As the optimal parameters of the maintenance process as for the condition the following was accepted: 1) a lot of facility's elements being maintained, 2) levels of maximum allowable values of the determining parameters of the elements being maintained, and 3) the frequency of monitoring the technical condition of the facility.

The target functions of the problem, that is the cost factor of maintenance and the average time between failures, are being obtained by using simulation statistical model. The problem is being solved approximately by using the developed software. A person-expert participates in the search for optimal solutions interactively. An example of solving the problem is given.

**Keywords:** maintenance, radio electronic equipment, exploiting

# СТРУКТУРИРОВАННОСТЬ СИГНАЛОГРАММ И УНИВЕРСАЛЬНОСТЬ ФРАКТАЛЬНОГО ПОДХОДА ПРИ СОЗДАНИИ ИНСТРУМЕНТАРИЯ ФОНОСКОПИЧЕСКОЙ ЭКСПЕРТИЗЫ

В.В. Журавель<sup>1</sup>, О.В. Рыбальский<sup>2</sup>, В.И. Соловьев<sup>3</sup>

<sup>1</sup> Государственный научно-исследовательский экспертно-криминалистический центр Министерства внутренних дел Украины,

ул. Большая Окружная, 4а, Киев, 03170, Украина; e-mail: fonoscopia@ukr.net

<sup>2</sup> Национальная академия внутренних дел,

пл. Соломенская, 1, Киев, 03035, Украина; e-mail: rybalsky\_ol@mail.ru

<sup>3</sup> Восточноукраинский национальный университет имени Владимира Даля,  
кв. Молодёжный, 20А, Луганск, 91034, Украина; e-mail: mettilyd@mail.ru

Рассмотрена задача построения комплекса методов и программного обеспечения проведения фоноскопической экспертизы, основанных на едином научном и методологическом подходе. Показана возможность построения такого комплекса инструментов на основе фрактального подхода.

**Ключевые слова:** экспертиза, цифровая фонограмма, цифровая видеозапись

## Введение

Появление и широкое внедрение во все области человеческой деятельности информационных технологий привело к существенному расширению возможностей изготовления поддельных фонограмм и видеозаписей фальсификаторами для достижения своих неблагоприятных целей.

С нашей точки зрения, наиболее опасны среди них две – создание фальсификатов для предоставления в следственные и судебные органы в качестве доказательной базы и предоставление фальшивок в СМИ или глобальную сеть для воздействия на общественное мнение.

Единственным противодействием таким проявлениям может быть фоноскопическая экспертиза. Однако ее проведение (да и само появление) также невозможно без использования информационных технологий. Это поясняется комплексом основных задач, решаемых такой экспертизой: идентификация диктора по физическим параметрам сигналов его речи; идентификация аппаратуры записи и проверка оригинальности и подлинности (отсутствие следов монтажа) фонограмм и видеозаписей, представленных на экспертизу.

Но в настоящее время в оснащении экспертов, производящих такие экспертизы, отсутствует полный комплекс методических и аппаратно-программных инструментов, предназначенных для их проведения, построенных на основе единого научно-обоснованного методологического и теоретического подхода. При этом, учитывая значительно возросшее количество экспертиз и увеличение объемов экспертных исследований, также весьма актуальна задача автоматизации самого процесса экспертизы.

## Цель статьи и постановка заданий

*Цель* настоящей работы – показать наличие единого научно-обоснованного методологического и теоретического подхода и обосновать возможность создания на его основе необходимого комплекса методических и аппаратно-программных инструментов проведения фоноскопической экспертизы.

Для достижения поставленной цели в работе решаются задачи:

- 1) Определение характерных структурных особенностей сигналов;
- 2) Выбор оптимального математического инструментария для выделения структурных составных частей сигналов;
- 3) Разработка специализированного программного обеспечения, реализующего предложенные методики экспертизы.

## Основная часть

Опубликованные нами работы и разработанные и внедренные в практику специализированные программы и методики их применения при идентификации цифровой аппаратуры звукозаписи в экспертизе оригинальности цифровых фонограмм [1, 2], навели нас на мысль о возможности применения использованных при их создании методологии и научного подхода для создания аналогичных инструментов проведения экспертизы цифровых фотографий и видеозаписей.

Результаты исследований в этом направлении оказались весьма продуктивными и, в конечном итоге, привели к созданию программы проведения идентификационных исследований цифровой фотоаппаратуры и диагностики оригинальности цифровых фотографий [3].

В основе разработанных программных средств и методик их применения лежит тот факт, что все эти сигналы носят фрактальный характер. Проведенный структурный анализ, подтвержденный многочисленными экспериментами, показал, что существуют четкая взаимосвязь между паразитными параметрами аппаратуры записи и индивидуальными характеристиками сигналов, фиксируемыми на носителе в процессе записи, выражаемая в образовании в сигналах самоподобных структур. Поэтому фрактальный подход к идентифицирующим признакам, выделяемых из исследуемых цифровых фонограмм, цветных фотографий и видеogramм (далее сигналограмм) идеально, по нашему мнению, подходит для создания необходимого инструментария.

Проведя некоторые обобщения, авторы пришли к выводу, что этот же подход вполне применим к идентификационным исследованиям личности диктора по физическим параметрам сигналов его устной речи. Поэтому сейчас проводится ряд исследований, первые результаты которых оказались весьма обнадеживающими (см., например, [4]).

В основании предложенного подхода лежит факт наличия устойчивых повторяющихся структур разного масштаба, носящих индивидуальный характер, как в сигналах собственных шумов цифровой аппаратуры записи информации, так и в сигналах речи. Эту структурированность можно увидеть во временной области при рассмотрении речевых сигналов, как это показано, например, на рис. 1.

В наличии фрактальности сигналов речи легко убедиться, рассмотрев вейвлет-портреты звукового сигнала, записанного на цифровом диктофоне, показанные на рис. 2. На них явно проглядываются ветвления исследуемых речевых сигналов, что является основным признаком их фрактальности.

Известно, что вейвлет-анализ является оптимальным инструментом для выделения самоподобных и мультифрактальных структур [5].

Учитывая свойства сигналов речи, записанных в цифровой форме, и собственных шумов цифровой аппаратуры записи, можно было предположить, что комплексный вейвлет Морле наиболее подходит для выделения из них таких структур.

Во временной области представление вейвлет-функции Морле [6]

$$\psi(t) = \pi^{-\frac{1}{4}} \left( e^{j\xi_0 t} - e^{-\frac{\xi_0^2}{2}} \right) e^{-\beta^2 t^2} = \pi^{-\frac{1}{4}} \left( e^{j\omega_c t} - e^{-\frac{\omega_c^2}{2}} \right) e^{-\frac{t^2}{2}}, \quad (1)$$

где

$$\beta = \frac{1}{\sqrt{2}};$$

$\omega_c$  – частота гетеродинирования гауссиана (носитель).

Его частотное представление определяется преобразованием Фурье от (1) и записывается [7] как

$$\Psi(j\omega) = \sqrt{2}\pi^{-\frac{1}{4}} \left( e^{-\frac{(\omega-\omega_c)^2}{2}} - e^{-\frac{\omega^2}{2}} e^{-\frac{\omega_c^2}{2}} \right). \quad (2)$$

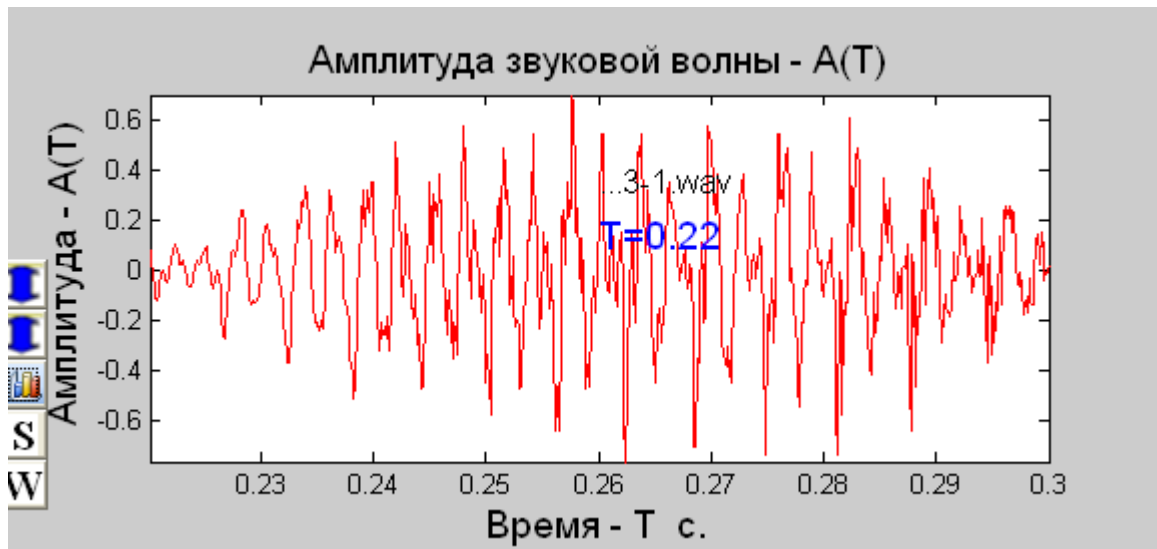
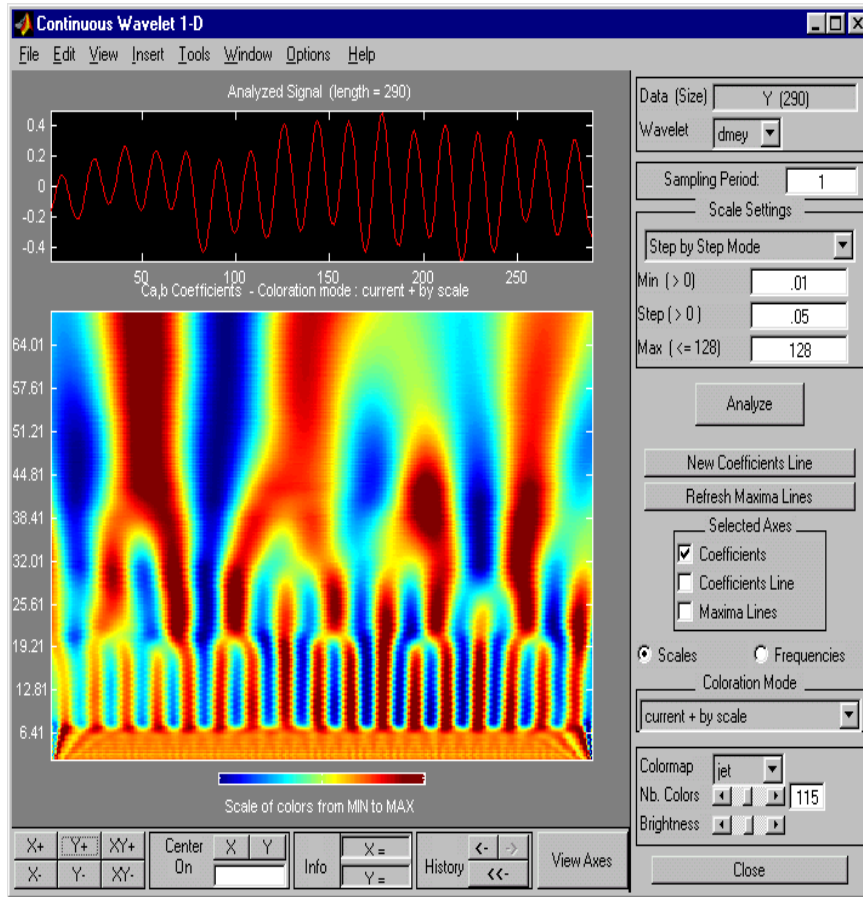
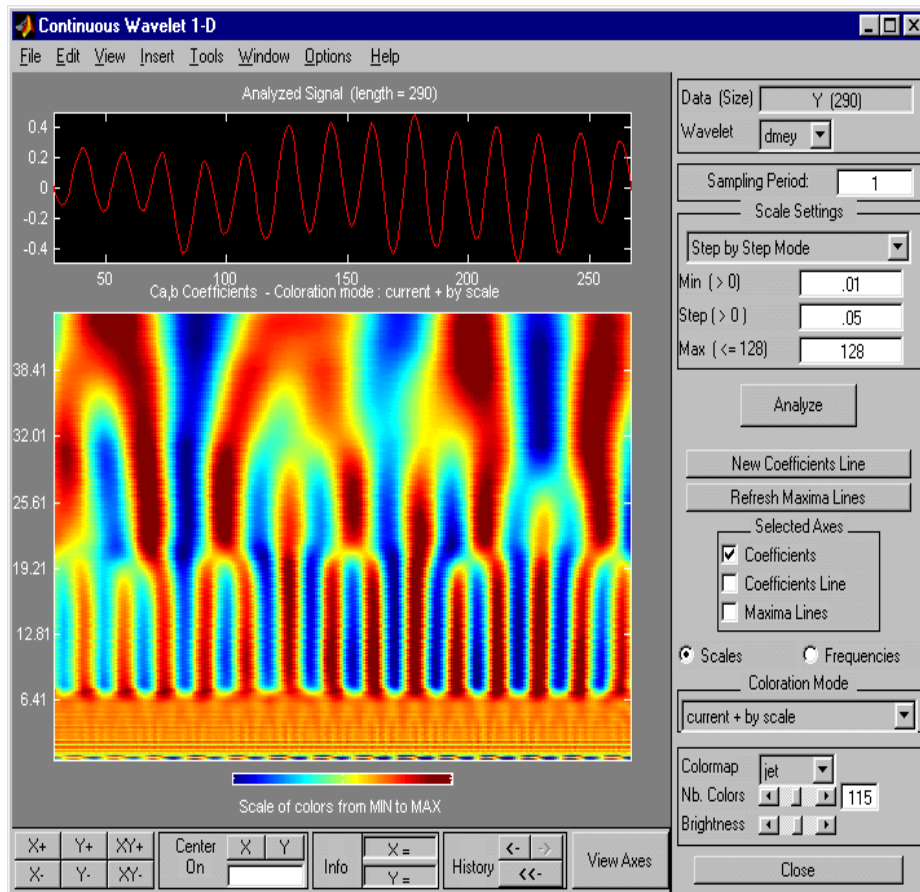


Рис. 1. График сигнала фрагмента речи

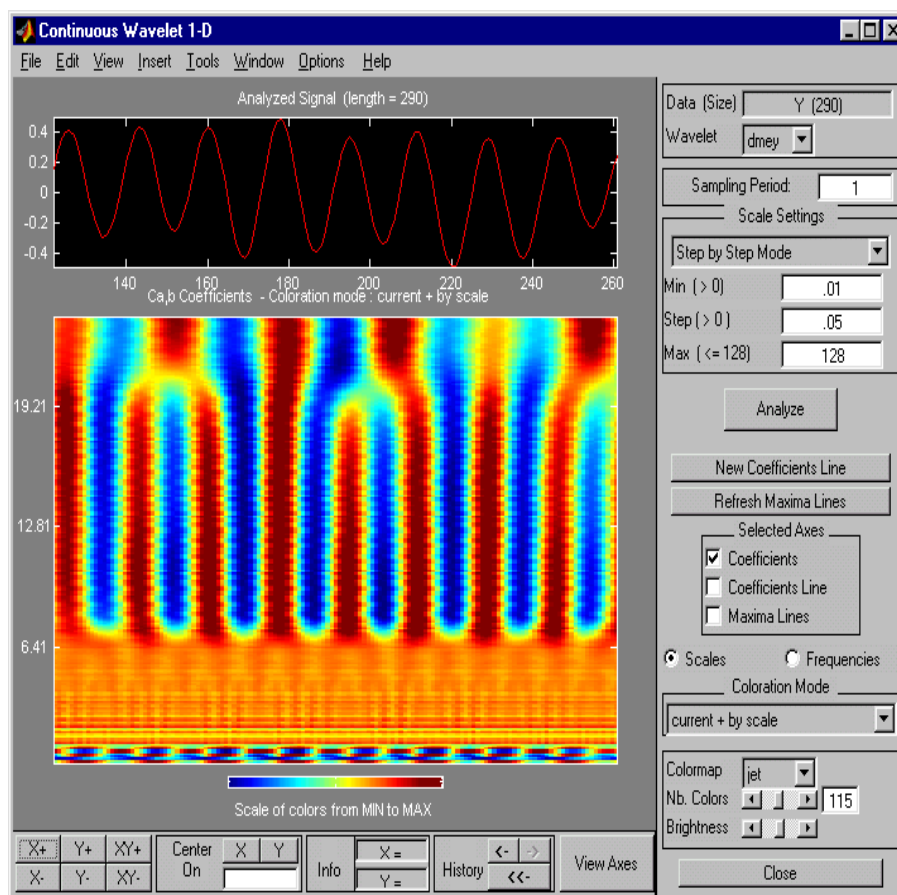


a



6





В

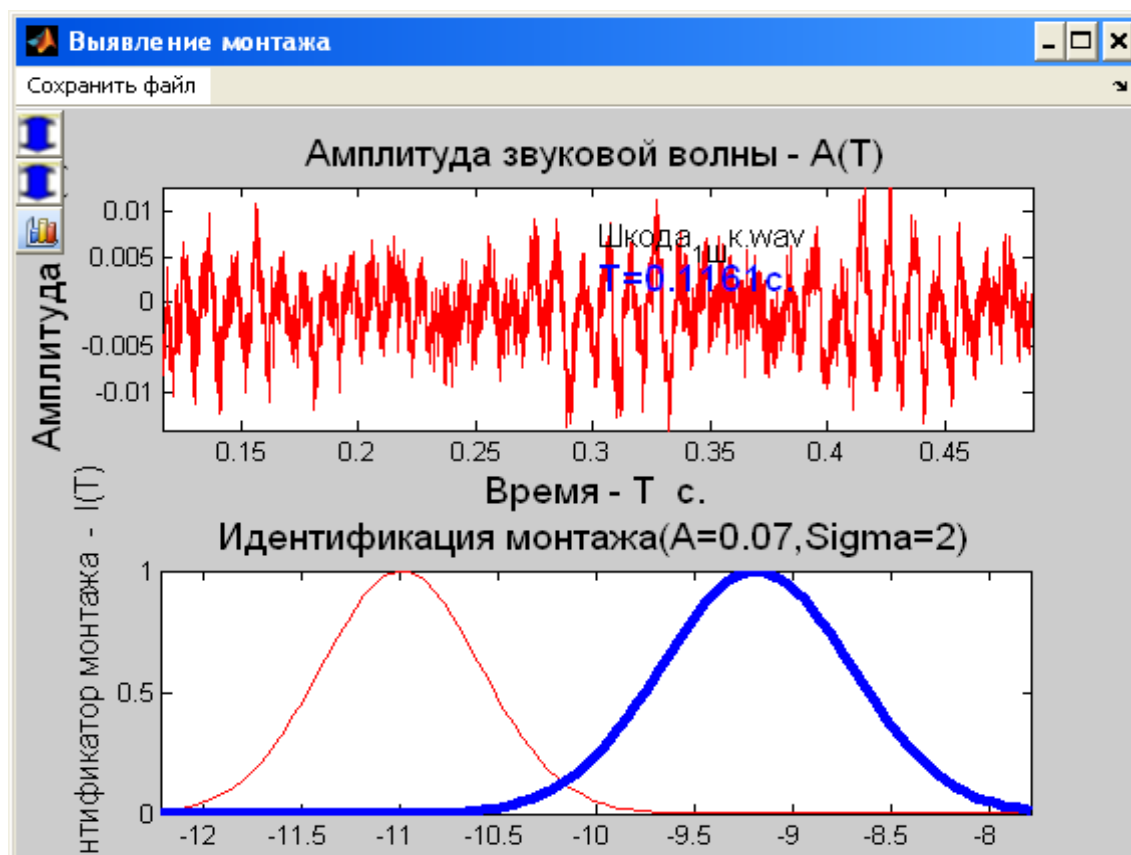
**Рис. 2.** Вейвлет-портрет модуля речевого сигнала, записанного и воспроизведенного при частоте дискретизации 8 кГц с 16-разрядной оцифровкой, полученный в программе *MathWorks* MATLAB: а – при малой детализации; б – при увеличении детализации; в – при последующем увеличении детализации

Этот вейвлет является гармоническим колебанием (носителем), промодулированным функцией Гаусса единичной ширины, и относится к так называемым прогрессивным вейвлетам. Так называют вейвлеты, спектр которых равен нулю для отрицательных значений пространственных частот. Они хорошо приспособлены для анализа процессов, подчиняющихся принципу причинности. Эти вейвлеты сохраняют направление движения времени и не создают паразитной интерференции между прошлым и будущим [8]. Поясняется это тем, что такие вейвлеты и, в частности, рассматриваемый нами вейвлет Морле, построены на гауссиане. Как известно, он обладает наилучшим соотношением разрешающей способности по частоте к разрешающей способности во времени (принцип неопределенности, т.е. невозможность одновременного определения мгновенной частоты сигнала и его значения в данный момент времени). Этими свойствами вейвлета Морле поясняется его теоретический выбор для решения рассматриваемых нами задач. Ранее, в работе [9] была экспериментально показана его оптимальность для вейвлет-анализа собственных шумов аппаратуры цифровой звукозаписи. В ряде последующих работ было показано, что особые свойства этого вейвлета наиболее пригодны для выделения из сигналов собственных шумов аппаратуры и сигналов речи самоподобных структур [3, 4, 10]. Поэтому при разработке программ для решения вышепоставленных задач экспертизы авторы использовали вейвлет Морле для выделения самоподобных структур.

При разработке программ необходимо решить ряд основных для них задач, например, задачу выделения пауз и автоматической сегментации речевого сигнала, задачу оптимизации выделения и учета самоподобных структур, задачу выделения основного тона и т.п. Большая часть этих задач на сегодня успешно решена (см., например, [10]).

Следует отметить, что при решении задачи выделения и учета самоподобных структур была использована идея минимального покрытия и индекса фрактальности, впервые предложенная в работе [8]. Их применение позволило, например, решить задачи выявления монтажа в паузах звукового сигнала (см. рис. 3) [10].

Однако при ее реализации потребовался ряд весьма существенных доработок и новых идей, связанных с нахождением, например, новых алгоритмов, обеспечивающих приемлемую вычислительную сложность проводимых расчетов. Но их рассмотрение не является предметом настоящей статьи.



**Рис. 3.** Распределение среднего значения амплитуды звуковой волны (пауза с монтажом)

Разумеется, что все приведенные работы опираются не только на теоретические исследования, но и экспериментальные данные, полученные в результате сотен проведенных экспериментов. При этом для их проведения было разработано свое специализированное программное обеспечение, ставшее основой для разработанных и разрабатываемых программ и методик экспертизы. Пример использования такого программного обеспечения показан на рис. 4.

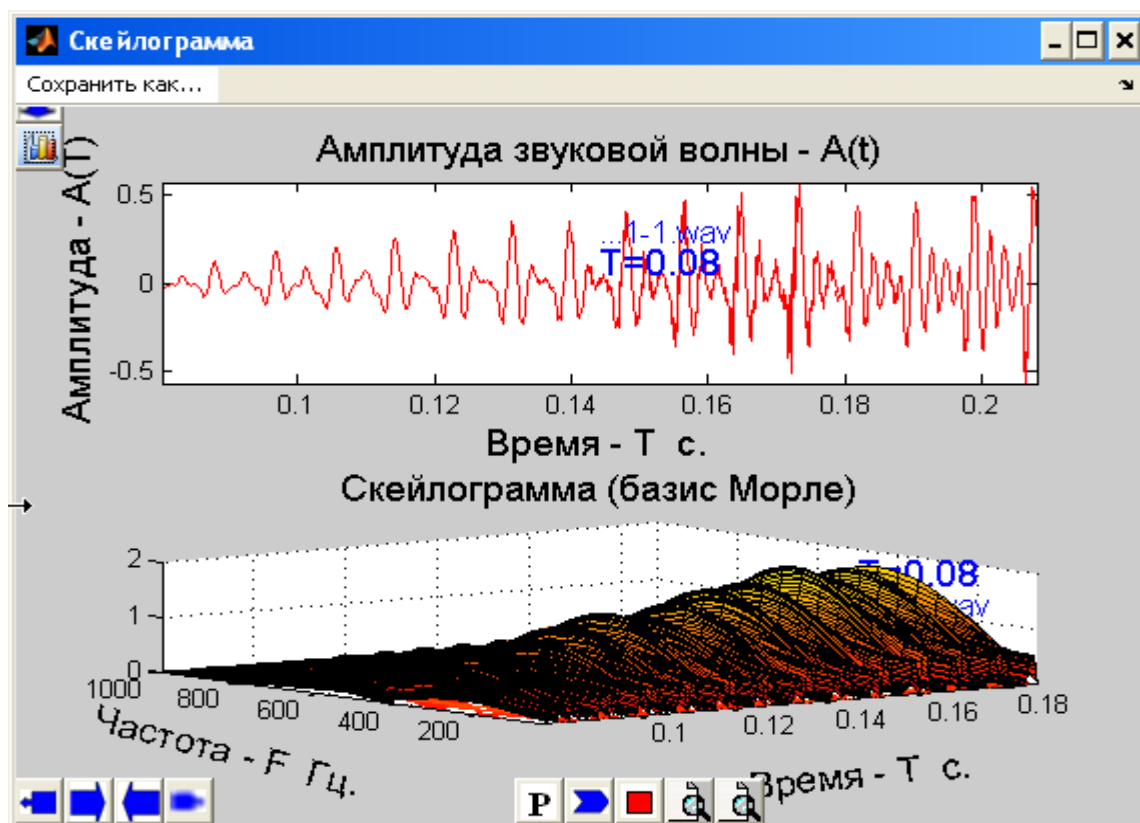


Рис. 4. Пример выявления и исследования самоподобных структур

## Выводы

Таким образом, можно отметить, что в настоящее время созданы все теоретические и экспериментальные предпосылки для разработки аппаратно-программного комплекса на основе фрактального подхода, предназначенного для проведения фоноскопической экспертизы в полном объеме решаемых в ней задач.

## Список литературы

1. Методика ідентифікаційних і діагностичних досліджень матеріалів та апаратури цифрового й аналогового звукозапису зі застосуванням програмного забезпечення «Фрактал» при проведенні експертиз матеріалів та засобів відео та звукозапису : наук.-метод. посіб. / О.В. Рыбальський, В.І. Соловйов, В.В. Журавель, Т.О. Татарнікова. — К. : ДУІКТ, 2013. — 75 с.
2. Соловьев, В.И. Идентификация аппаратуры аудиозаписи по статистическим характеристикам аудиофайлов / В.И. Соловьев // Реєстрація, зберігання і обробка даних. — 2013. — Том 15, № 1. — С. 59–70.
3. Рыбальский, О.В. Программа идентификации цифровой фото- и видеоаппаратуры и проверки оригинальности цифровых изображений / О.В. Рыбальский, В.И. Соловьев, Е.В. Белозеров // Вісник Київського національного університету ім. Т. Шевченка. Військово-спеціальні науки. — 2013. — Вип. 41. — С. 77–80.
4. Соловьев, В.И. Идентификация характеристик голоса на основе максимумов вейвлет-преобразования / В.И. Соловьев // Реєстрація, зберігання і обробка даних. — 2013. — Том 15, № 2. — С. 39–47.
5. Малла, С. Вэйвлеты в обработке сигналов = A wavelet tour of signal processing : учеб. пособие для вузов по специальности 010200 «Прикладная математика и информатика» и по

- направлению 510200 «Прикладна математика и информатика» / С. Малла ; пер. со второго англ. изд. Я.М. Жилейкина. — М. : Мир, 2005. — 671 с.
6. Геранін, В.О. Математичні аспекти хвильового аналізу [Текст] : навч. посібник з 16 лекцій: Для студ. вищих навч. закл. / В.О. Геранін [та ін] ; Національний технічний ун-т України «Київський політехнічний ін-т». — К. : ВПФ УкрІНТЕІ, 2001. — 160 с.
  7. Рыбальский, О.В. К вопросу о представлении вейвлет-функции Морле в частотной области / О.В. Рыбальский // Вісник Східноукраїнського національного університету імені Володимира Даля. — 2007. — № 5(111), Ч. 1. — С. 104–106.
  8. Старченко, Н.В. Локальный анализ хаотических временных рядов с помощью индекса фрактальности : автореф. дис. на соискание уч. степени канд. физ.-мат. наук : спец. 05.13.18 «Математическое моделирование, численные методы и комплексы программ», 01.01.03 «Математическая физика» / Н.В. Старченко. — Москва, 2005. — 20 с.
  9. Рыбальский, О.В. Выявление признаков обработки цифровых фонограмм с помощью вейвлет-анализа сигналов / О.В. Рыбальский, Т.В. Мовчан, Л.Д. Писаренко, Ю.В. Путилов // Рестрація, зберігання і обробка даних. — 2002. — Том 4, № 3. — С. 89–103.
  10. Соловьев, В.И. Локализация следов обработки сигнала в задачах монтажа аудиозаписи / В.И. Соловьев, О.В. Рыбальский, В.К. Железняк // Вестник Полоцкого государственного университета. Сер. С, Фундаментальные науки. — 2013. — № 4. — С. 5–11

## СТРУКТУРОВАНІСТЬ СИГНАЛОГРАМ ТА УНІВЕРСАЛЬНІСТЬ ФРАКТАЛЬНОГО ПІДХОДУ ПРИ СТВОРЕННІ ІНСТРУМЕНТАРНО ФОНОСКОПІЧНИХ ЕКСПЕРТИЗ

В.В. Журавель<sup>1</sup>, О.В. Рыбальський<sup>2</sup>, В.І. Соловйов<sup>3</sup>

<sup>1</sup> Державний науково-дослідний експертно-криміналістичний центр Міністерства внутрішніх справ України,

вул. Велика Окружна, 4а, Київ, 03170, Україна; e-mail: fonoscopia@ukr.net

<sup>2</sup> Національна академія внутрішніх справ,

пл. Солом'янська, 1, Київ-ДСП, 03035, Україна; e-mail: rybalsky\_ol@mail.ru

<sup>3</sup> Східноукраїнський національний університет імені Володимира Даля, кв. Молодіжний, 20А, Луганськ, 91034, Україна; e-mail: mettilyd@mail.ru

Розглянуто завдання побудови комплексу методів і програмного забезпечення проведення фоновскопичної експертизи, заснованих на єдиному науковому і методологічному підході. Показана можливість побудови такого комплексу інструментів на основі фрактального підходу.

**Ключові слова:** експертиза, цифрова фонограма, цифрова відеограма

## SIGNALOGRAMM STRUCTURE AND UNIVERSALITY OF THE FRACTAL APPROACH TO THE DEVELOPMENT OF THE PHONOSCOPE ASSESSMENT TOOLKIT

Vadim V. Zhuravel<sup>1</sup>, Oleg V. Rybalsky<sup>2</sup>, Viktor I. Solovyev<sup>3</sup>

<sup>1</sup> State research expertly-criminalistics center of Ministry of Internal Affairs of Ukraine, 4A Velyka Okruzhna str., Kyiv, 03170, Ukraine; e-mail: fonoscopia@ukr.net

<sup>2</sup> National Academy of Internal Affairs,

1 Solomenskaya sqr., Kyiv, 03035, Ukraine; e-mail: rybalsky\_ol@mail.ru

<sup>3</sup> Volodymyr Dhal East Ukraine National University, 20-A Molodizhnyi kvartal, Luhansk, 91034, Ukraine; e-mail: mettilyd@mail.ru

The task of construction of complex of methods and realization of fono examination software is considered, based on single scientific and methodological approach. Possibility of construction of such complex of instruments is shown on the basis of fractal approach

**Keywords:** assessment, digital phonogram, digital videogram

## МЕТОДИЧНІ ЗАСАДИ ЗАСТОСУВАННЯ НЕЙРОМЕРЕЖ У ЗАДАЧАХ ПРОГНОЗУВАННЯ ТА КЕРУВАННЯ

С.В. Ленков<sup>1</sup>, В.М. Штепа<sup>2</sup>, А.О. Дудник<sup>2</sup>, А.С. Шворов<sup>3</sup>

<sup>1</sup> Військовий інститут Київського національного університету імені Тараса Шевченка,  
вул. Ломоносова, 81, Київ, 03680, Україна; e-mail: lenkov\_s@ukr.net

<sup>2</sup> Національний університет біоресурсів і природокористування України,  
вул. Героїв Оборони, 15, Київ, 03041, Україна; e-mail: dudnikalla@mail.ua

<sup>3</sup> Військова частина К1410,  
Україна

Описано процедуру синтезу методики нейромережевого (НМ) прогнозування зовнішніх збурень на об'єкт спеціального призначення (ОСП). Проведено порівняння прогнозування часових рядів температури навколишнього середовища з використанням типового підходу (градієнтний метод) щодо оптимізації значень вагових коефіцієнтів нейронної мережі та із застосуванням генетичного алгоритму. Досліджено якість роботи системи керування з блоком нейромережевого прогнозування та оптимізацією його налаштувань на основі використання генетичного алгоритму порівняно із системою без такого прогнозування. Встановлено, що вирішення завдання математичного моделювання проєкцій часових рядів дозволяє значно підвищити швидкість системи керування та забезпечити максимальну ефективність функціонування ОСП.

**Ключові слова:** нейромережеве прогнозування, збурення, система керування

### Вступ

Значні витрати палива на обігрів ОСП зумовлені декількома причинами, основними з яких є низькі теплозахисні властивості огорожуючих конструкцій та недосконала робота систем опалення. У зв'язку з високою вартістю енергоресурсів важливого значення та актуальності набуває розробка нових комплексних рішень, реалізація яких дозволить значно зменшити витрати енергії на обігрів ОСП. Доцільним вбачається врахування прогнозованих значень зовнішніх збурень на процес керування обігрівом ОСП з метою підвищення ефективності його функціонування. Для вирішення цього завдання виникає необхідність у розробці методики нейромережевого прогнозування зовнішніх збурень на процес обігріву ОСП.

### Мета дослідження

Розробити методику нейромережевого прогнозування зовнішніх збурень на процес обігріву ОСП, дослідити ефективність такого підходу.

### Викладення основного матеріалу дослідження

Основними факторами зовнішнього середовища, що впливають на процес обігріву ОСП, є температура та інтенсивність сонячної радіації [3, 5]. Оптичне

випромінювання впливає на тепловий режим споруд і є важливим фактором, що також необхідно враховувати в тепловому балансі споруд ОСП.

Інформація щодо значень параметрів мікроклімату та збурюючих впливів на ОСП була отримана з використанням інформаційно-виміральної системи (ІВС), яка розроблена із застосуванням датчиків температури, вологості та інтенсивності сонячної радіації, та змонтована на території Броварського району Київської області.

На основі статистичних даних, отриманих за допомогою ІВС, застосовувалась методика прогнозування часових рядів температури [4] з використанням нейромережових технологій [2].

Для синтезу та дослідження НМ використовувався програмний пакет Statistica Neural Networks. З метою отримання прогнозованих значень для температурного часового ряду прийнятна точність предикатів була отримана за допомогою багатощарового перцептронну з двома нейронами у прихованому шарі (рис. 1).

Подальші дослідження були спрямовані на пошук оптимізаційних алгоритмів для підвищення точності предикатів. Серед оптимізаційних математичних апаратів у контексті поставленої задачі виділяється генетичний алгоритм (ГА).



**Рис. 1.** Графіки прогнозування температурних часових рядів

Суть методу полягає в налаштуванні вагових коефіцієнтів нейронної мережі шляхом випадкового перехресчування хромосом до тих пір, поки не буде знайдене оптимальне рішення. Розв'язку задачі відповідає хромосома з мінімальним значенням функції належності, що визначає оптимальний вектор вагових коефіцієнтів  $W_i$ , при цьому похибка навчання менша заданої величини  $\varepsilon_{\min}$  [1].

Класично для навчання нейронних мереж використовувався наступний алгоритм:

- 1) Задаються деякі  $\eta$  ( $0 < \eta < 1$ ),  $E_{\max}$  і деяка мала випадкова вага  $w_i$  мережі.
- 2) Задаються  $k = 1$  і  $E = 0$ .
- 3) Вводиться чергова навчальна пара  $(x^k, y^k)$ .

Проводяться позначення

$$x := x^k, \quad y := y^k,$$

обчислюється величина виходу мережі:

$$o = o(w^T x) = \frac{1}{1 + e^{-w^T x}}. \quad (1)$$

- 4) Обновляється (корегується) вага:

$$w := w + \eta(y - o)o(1 - o)x. \quad (2)$$

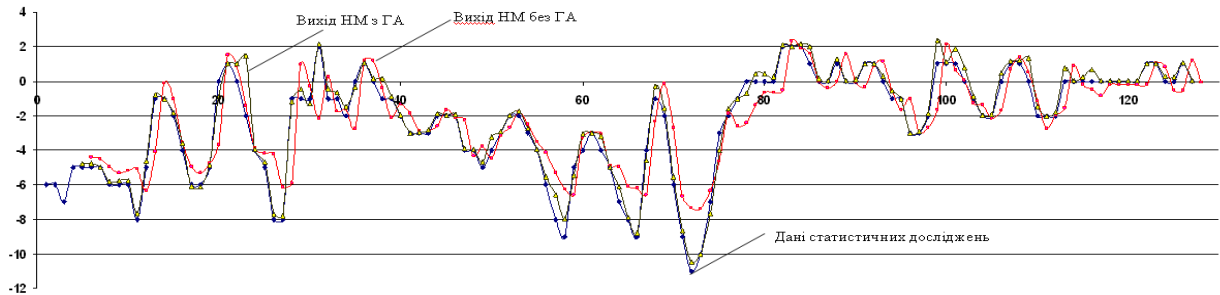
5) Корегується (нарощується) значення функції помилки:

$$E := E + \frac{1}{2}(y - o)^2. \quad (3)$$

6) Якщо  $k < N$ , тоді  $k := k + 1$  і перехід до кроку 3, у протилежному випадку – перехід до кроку 7.

7) Завершення циклу навчання. Якщо  $E < E_{\max}$ , то закінчується процедура навчання. Якщо  $E \geq E_{\max}$ , тоді починається новий цикл навчання переходом до кроку 2.

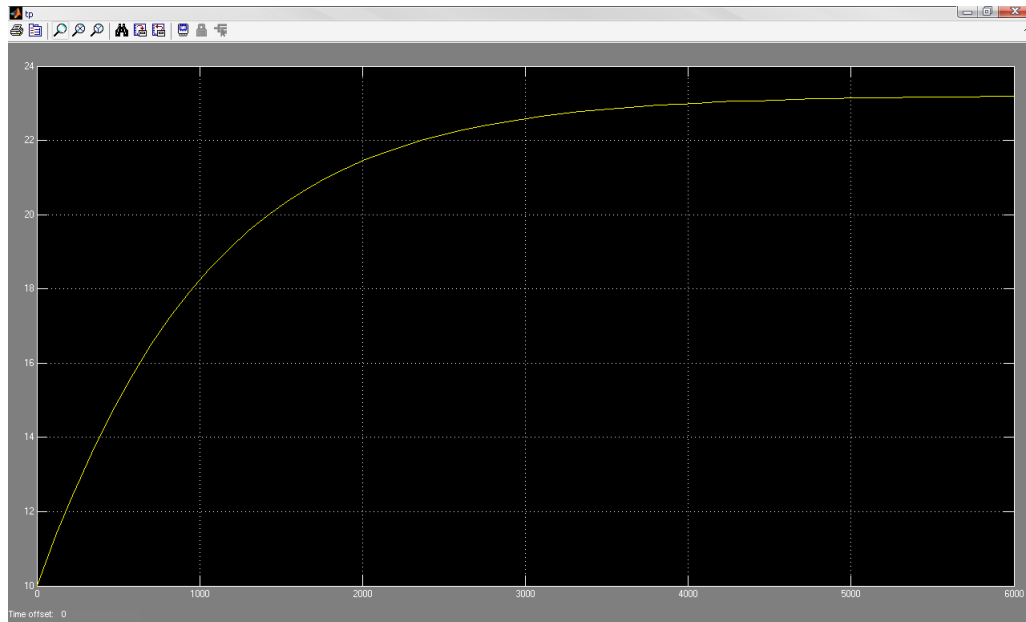
Паралельно визначалися оптимальні вагові коефіцієнти нейронної мережі типу багатoshаровий перцептрон для температурного часового ряду за допомогою генетичного алгоритму. Аналізуючи проєкції часових рядів температури (рис. 2), необхідно відмітити, що НМ відносно вірно спрогнозували її зниження, збільшення та стабілізацію. При прогнозуванні на 12 годин вперед в цілому спостерігається підвищення точності прогнозу нейронною мережею з використанням генетичного алгоритму (середньоквадратична помилка – 0.53641 °C), порівняно із звичайною нейронною мережею (середньоквадратична помилка – 1.007193 °C).



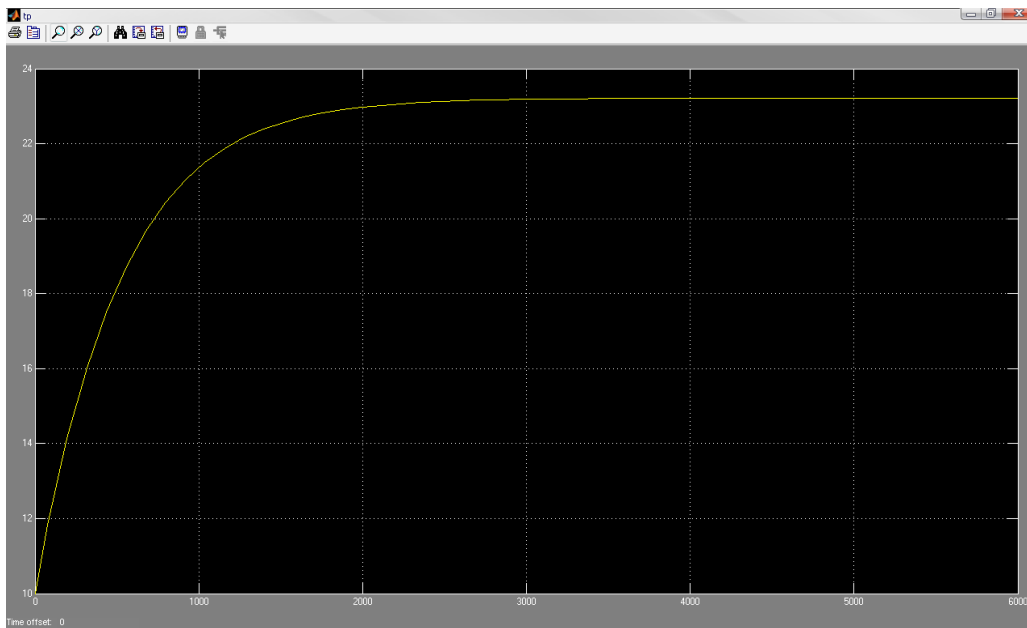
**Рис. 2.** Графіки навчального прогнозування температурних часових рядів нейронними мережами

З метою визначення ефективності прогнозування зовнішніх збурень у вигляді температури проведено порівняльне дослідження часу регулювання, тобто періоду, за який температура в теплиці досягне усталеного значення. Спочатку виконувались дослідження системи керування, яка не містить блоку прогнозування зовнішніх природних збурень. Для такої системи час регулювання змінювався в межах від 4010 до 5150 секунд в залежності від температури повітря ззовні теплиці. Дослідження системи керування, яка містить блок прогнозування, показали зміну часу регулювання в межах 3600 – 4100 с, що значно менше від системи першого типу.

На рис. 3 показані розгінні криві процесу нагріву температури повітря в ОСП, отримані з використанням імітаційної моделі. Так, для досягнення температури повітря 23°C система стабілізується за 5150 с (рис. 3(а)). Імітаційне моделювання системи керування, що містить блок прогнозування, показало, що усталене значення температури повітря буде досягнуто за час 4100 с (рис. 3(б)), що майже на 21% менше в порівнянні з існуючою системою керування.



а



б

**Рис. 3.** Розгінні криві для температури повітря в ОСП при зовнішній температурі повітря  $-15^{\circ}\text{C}$ : а — система керування без блоку прогнозування зовнішніх збурень, б — система керування з блоком прогнозування збурень

У таблиці 1 наведено результати імітаційного дослідження системи керування за часом регулювання внутрішньої температури повітря в ОСП, залежно від зовнішніх збурень (у вигляді температури повітря).



Таблиця 1.

Результати моделювання часу регулювання для систем керування різних типів

| Зовнішні збурення |                               | Змінна керування              | Ефективність систем керування за часом регулювання |                          |                             |
|-------------------|-------------------------------|-------------------------------|--|--------------------------|-----------------------------|
| Температура, °С   | Температура повітря в ОСП, °С | Температура повітря в ОСП, °С | Час регулювання (1)*, с                            | Час регулювання (2)**, с | Коефіцієнт ефективності $K$ |
| -15               | 500                           | 18.5                          | 4010   | 3600                     | 10.22                       |
| -10               | 400                           | 19.5                          | 4300   | 3200                     | 25.58                       |
| -5                | 600                           | 20.5                          | 4500   | 3400                     | 24.44                       |
| 5                 | 700                           | 22.5                          | 4800   | 3600                     | 25.00                       |
| 10                | 350                           | 23                            | 5150   | 4100                     | 20.39                       |

\* система керування, що працює за алгоритмом стабілізації параметрів (без прогнозування збурень);

\*\* система керування з нейромережовим прогнозуванням збурень

Ефективність системи керування за часом регулювання визначалась за виразом (1):

$$K = \frac{(T_p - T_{op})}{T_p} \times 100\% \quad (4)$$

Показник ефективності  $K$  показує, на скільки відсотків зменшиться час регулювання в системі керування з прогнозуванням збурень порівняно з системою стабілізації параметрів.

На основі отриманих результатів побудовано графік залежності часу регулювання температури в ОСП в залежності від зовнішньої температури повітря (рис. 4).

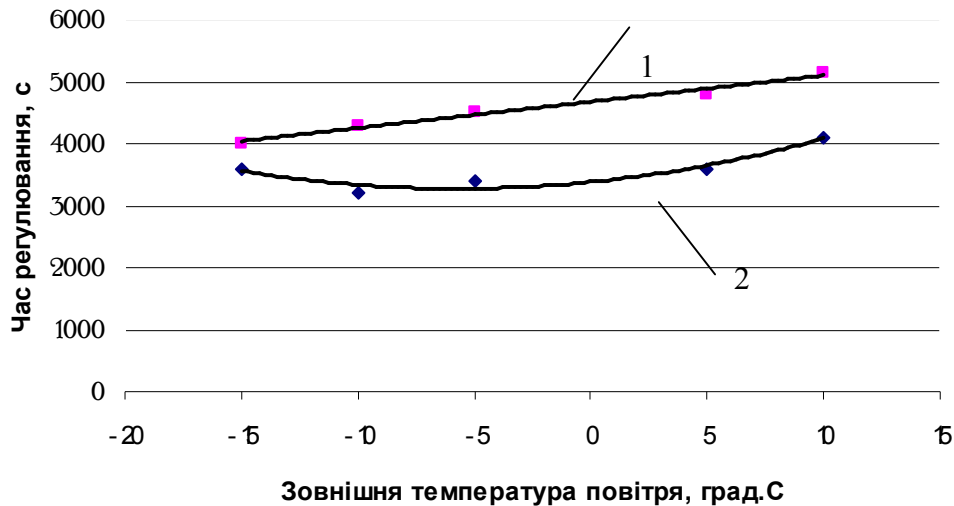


Рис. 4. Зміна часу регулювання залежно від зовнішньої температури повітря: 1 — система керування без прогнозування збурень; 2 — система керування з прогнозуванням збурень

## Висновки

Розроблена методика нейромережевого прогнозування зовнішніх збурень на ОСП дозволяє підвищити швидкодію системи керування і відповідно забезпечує підвищення технологічної ефективності функціонування ОСП.

## Список літератури

1. Заєць, Н.А. Використання генетичного алгоритму для вирішення оптимізаційних задач в електротехніці / Н.А. Заєць, В.М. Штепа // Науковий вісник Національного університету біоресурсів і природокористування України. Серія: Техніка та енергетика АПК. — К. : НУБіПУ, 2011. — Вип. 166, Ч. 4. — С. 157–164.
2. Каллан, Р. Основные концепции нейронных сетей / Р. Каллан; [пер. с англ. и ред.: Сивака А.Г.]. — М. [и др.] : Вильямс, 2001. — 287 с.
3. Клешнин, А.Ф. Растение и свет. Теория и практика светокультуры растений [Текст] : научное издание / А.Ф. Клешнин ; Акад. наук СССР, Ин-т физиологии растений им. К.А. Тимирязева. — М. : Изд-во Акад. наук СССР, 1954. — 456 с.
4. Отнес, Р. Прикладной анализ временных рядов. Основные методы [Текст] : научное издание / Р. Отнес, Л. Эноксон ; пер. с англ. В.И. Хохлова ; ред. И.Г. Журбенко. — М. : Мир, 1982. — 428 с.
5. Hurd, R.G. An Analysis of the Growth of Young Tomato Plants in Water Culture at Different Light Integrals and CO<sub>2</sub> Concentrations II. A Mathematical Model / R.G. Hurd, J.H.M. Thornley // Annals of Botany. — 1974. — Vol. 38, Iss. 2. — PP. 389–400.

**МЕТОДИЧЕСКИЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ НЕЙРОННЫХ СЕТЕЙ В ЗАДАЧАХ ПРОГНОЗИРОВАНИЯ И УПРАВЛЕНИЯ**

С.В. Ленков<sup>1</sup>, В.Н. Штепа<sup>2</sup>, А.А. Дудник<sup>2</sup>, А.С. Шворов<sup>3</sup>

<sup>1</sup> Военный институт Киевского национального университета имени Тараса Шевченко, ул. Ломоносова, 81, Киев, 03680, Украина; e-mail: lenkov\_s@ukr.net

<sup>2</sup> Национальный университет биоресурсов и природопользования, ул. Героев Обороны, 15, Киев, 03041, Украина; e-mail: dudnikalla@mail.ua

<sup>3</sup> Военная часть К1410, Украина

Описана процедура синтеза методики нейросетевого прогнозирования внешних возмущений на объект специального назначения (ОСН). Проведено сравнение прогнозирования временных рядов температуры окружающей среды с использованием типового подхода (градиентный метод) по оптимизации значений весовых коэффициентов нейронной сети и с помощью генетического алгоритма. Исследовано качество работы системы управления с блоком нейросетевого прогнозирования и оптимизацией его настроек на основе генетического алгоритма по сравнению с системой без такого прогнозирования. Установлено, что решение задачи математического моделирования проекций временных рядов позволяет значительно повысить быстродействие системы управления и обеспечить максимальную эффективность функционирования ОСН.

**Ключевые слова:** нейросетевое прогнозирование, возмущения, система управления

**METHODOLOGICAL BASIS OF NEURAL NETWORKS APPLICATIONS FOR FORECASTING AND MANAGEMENT TASKS**

Sergey V. Lenkov<sup>1</sup>, Volodymyr M. Shtepa<sup>2</sup>, Alla O. Dudnik<sup>2</sup>, Andriy S. Shvovor<sup>3</sup>

<sup>1</sup> Military Institute, Taras Shevchenko National University of Kyiv, 81 Lomonosov str., Kyiv, 03680, Ukraine; e-mail: lenkov\_s@ukr.net

<sup>2</sup> National University of Life and Environmental Sciences, 15 Heroiv Oborony str., Kyiv, 03041, Ukraine; e-mail: dudnikalla@mail.ua

<sup>3</sup> K1410 Military Unit, Ukraine

The procedure for the synthesis method of neural network prediction of external perturbations on the special-purpose entity (SPE) is presented. A comparison of the time series forecasting ambient temperature using a typical approach (gradient method) to optimize the weighting coefficients of the neural network and genetic algorithm. Investigated the quality of the system control unit neural network prediction and optimization of its configuration based on genetic algorithm compared to a system without such a prediction. Found that the solution to the problem of mathematical modeling of time series of projections can significantly improve the performance of the control system and to maximize the efficiency of the SPE.

**Keywords:** neural network forecasting, disturbance, control system

# ИНФОРМАЦИОННАЯ КОГНИТИВНАЯ МОДЕЛЬ ТЕХНОЛОГИЧЕСКОЙ ВЗАИМОЗАВИСИМОСТИ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ

Н.Д. Рудниченко, В.В. Вычужанин

Одесский национальный морской университет,  
ул. Мечникова, 34, Одесса, 65404, Украина; e-mail: rudnick@mail.ua

В статье приведены результаты исследований разработанной информационной когнитивной модели технологической взаимозависимости и взаимосвязи сложных технических систем для оценки их уязвимости. Построена общая структурная схема взаимосвязанности судовых сложных технических систем. Исследовано взаимодействие агрегатов судовой энергетической установки, системы энергоснабжения судна и судовых вспомогательных систем в аварийных экстремальных ситуациях. На основании полученных результатов исследований разработана информационная когнитивная модель технологической взаимозависимости функционирования судовых сложных технических систем. В соответствии с созданным алгоритмом оценки уязвимости элементов информационной когнитивной модели произведен расчет коэффициентов структурной уязвимости ее элементов. Результаты расчета позволили определить наиболее критичные по надежности элементы модели. Полученные результаты исследований и разработок позволяют повысить эффективность эксплуатации сложных технических систем, обеспечить качественное прогнозирование надежности их функционирования в аварийных экстремальных ситуациях.

**Ключевые слова:** взаимозависимость, взаимосвязь, когнитивное моделирование, надежность, система поддержки и принятия решений

## Введение

Сложные технические системы (СТС), функционирование которых характеризуется взаимозависимостью и взаимосвязностью, обладают повышенным риском в работе, связанным с подверженностью разного рода аварийным ситуациям. Для надежной работы таких СТС крайне важно оперативное принятие управляющих решений по прогнозированию и минимизации негативных последствий от аварийных ситуаций. В этих целях возможно использование системного подхода при оценке надежности функционирования СТС, учитывающего взаимозависимость и взаимосвязность подобных систем. Основой системного подхода может стать разработка и использование когнитивных моделей, позволяющих выявить противоречия совместного функционирования СТС, осуществить их качественный анализ, разработать структурную схему причинно-следственных связей ключевых агрегатов исследуемой технической системы [1–5]. Когнитивное моделирование различных сценариев развития позволяет рассмотреть варианты развития ситуации при различных условиях, оценить возможность достижения целей. Благодаря этому становится возможной разработка оптимальной стратегии управления СТС.

Первым этапом разработки когнитивной модели технологической взаимозависимости и взаимосвязи СТС должна стать формулировка целей (предназначения) деятельности технических систем. Так СТС, установленные на судах,

должны обеспечить требуемые мореходные качества судов, поддержание заданных параметров их функционирования. Спецификой функционирования технологически взаимозависимых и взаимосвязанных судовых СТС является то, что в условиях постоянных внешних и внутренних воздействий, посредством согласованной работы систем производится передача и обмен информацией, энергией, а также жидкими, газообразными и многофакторными веществами, позволяющих судну успешно функционировать.

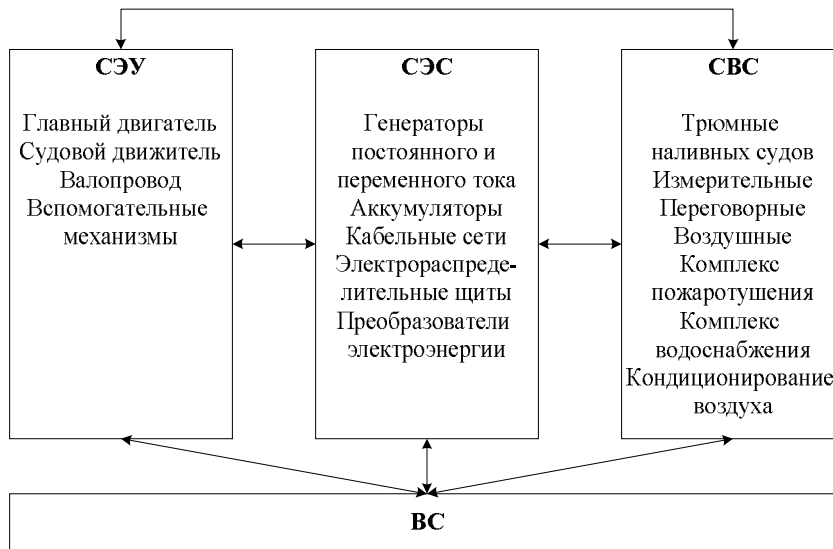
### **Цель статьи и постановка исследований**

*Целью* статьи является разработка и исследование информационной когнитивной модели технологической взаимозависимости и взаимосвязи судовых комплексов технических систем (СКТС) для оценки и обеспечения прогнозирования надежности оборудования судов в аварийных экстремальных ситуациях.

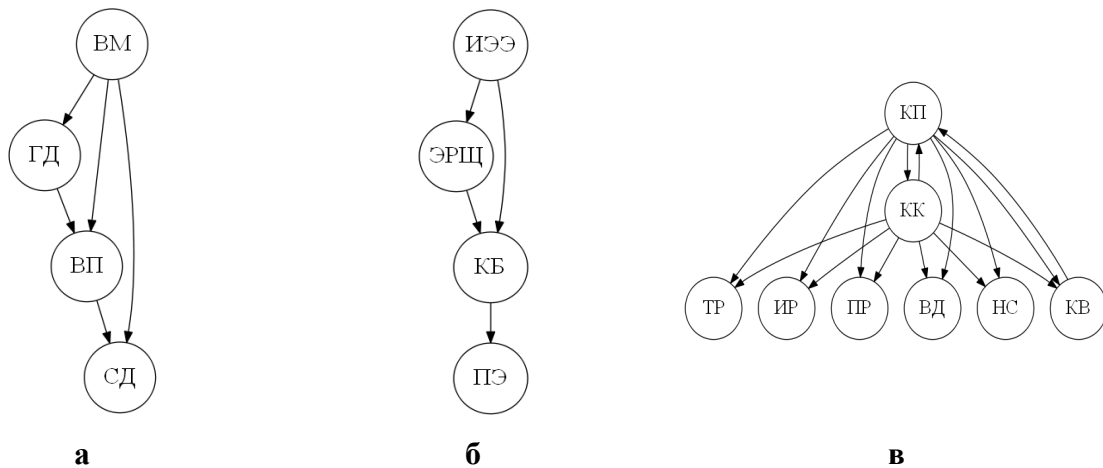
Для успешного проведения исследований предлагается представить оборудование судна совокупностью систем, состоящих из взаимозависимых и взаимосвязанных наиболее значимых СТС: судовая энергетическая установка (СЭУ); система энергоснабжения судна (СЭС); судовые вспомогательные системы (СВС). При проведении исследований необходимо учесть воздействия внешней окружающей среды (ВС), как совокупность сложно прогнозируемых природных и неприродных факторов в аварийных экстремальных ситуациях.

### **Изложение основного материала исследования**

Основными структурными объектами СЭУ являются: главный двигатель (ГД), судовой движитель (СД), валопровод (ВП), а также вспомогательные механизмы (ВМ). СЭС состоит из источников электрической энергии (ИЭЭ) в виде генераторов постоянного и переменного тока, аккумуляторов, кабельных сетей (КБ), электрораспределительных щитов (ЭРЩ), преобразователей электроэнергии (ПЭ). СВС представляют собой комплекс различных систем, основными из которых являются: трюмная (ТР); балластная (БС); пожаротушения – комплекс пожаротушения (КП); комфортного кондиционирования воздуха, технического кондиционирования воздуха, парового отопления – климатический комплекс (КК). Для выбранного состава СКТС структурная схема взаимозависимости и взаимосвязанности систем имеет вид, представленный на рис. 1. В когнитивной модели СКТС учтено взаимодействие и взаимосвязи агрегатов, находящихся в каждой подсистеме СЭУ, СЭС и СВС (рис. 2).

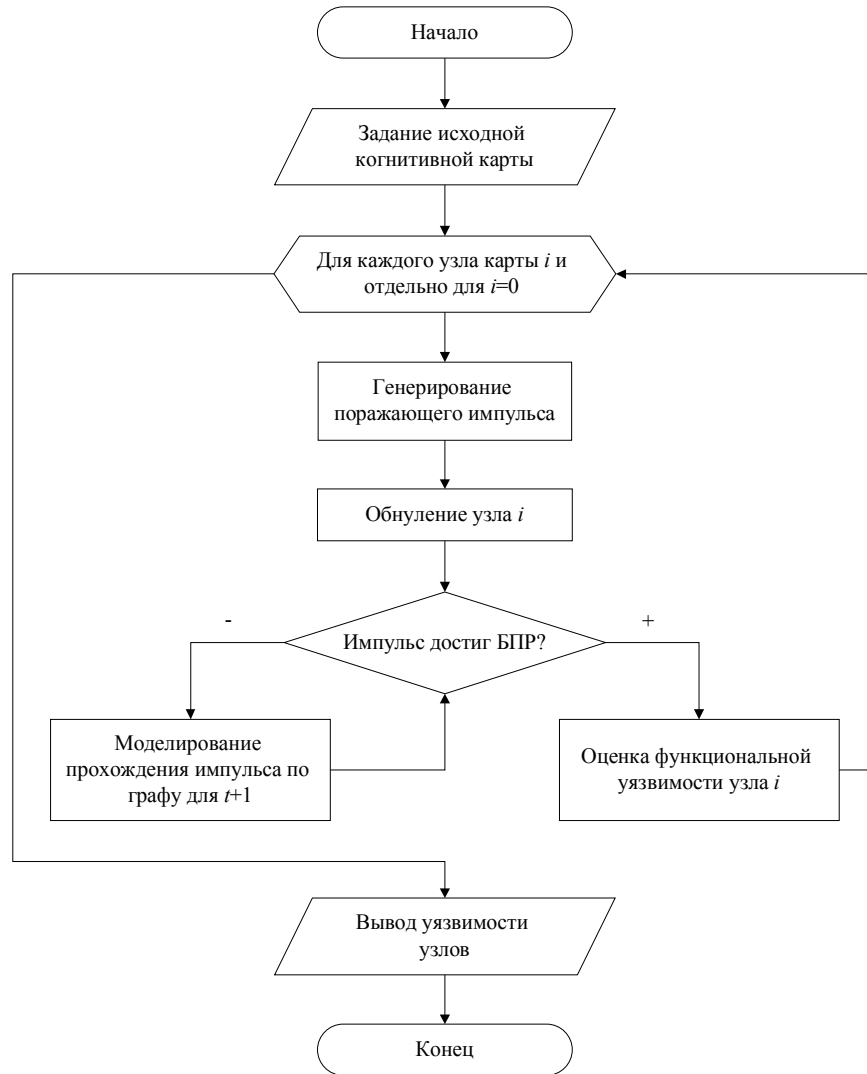


**Рис 1.** Структурная схема взаимозависимости и взаимосвязанности СКТС



**Рис 2.** Взаимодействие и взаимосвязи агрегатов модели СКТС: а – взаимодействие объектов подсистемы СЭУ; б – взаимодействие объектов подсистемы СЭС; в – взаимодействие объектов подсистемы СВС

При разработке когнитивной модели использован язык DOT, служащий для описания и построения графов модели. Интерпретация кода произведена с использованием программного продукта *Graphviz*. Моделирование осуществлено в соответствии с алгоритмом, приведенным на рис. 3.



**Рис. 3.** Алгоритм оценки уязвимости узлов

Согласно когнитивной карте взаимозависимых и взаимосвязанных судовых технических средств (рис. 4), первоначальное воздействие на судно оказывается внешней средой. При проведении исследований импульс поражающего воздействия, связанный с факторами внешней среды, перемещается к ключевым элементам каждой из подсистем. Проходя по соответствующим связям через все агрегаты СКТС, поражающий импульс поступает на блок приемника (БПР), предназначенный для анализа состояния работоспособности каждой подсистемы комплекса. Ключевые элементы подсистем СЭУ и СЭС на рис 6 обозначены двойными окружностями.

При моделировании дополнительно использовался подход, заключающийся в аналитическом или экспертном выборе соответствующих вершин графа, на которые производится моделирующее воздействие, а также моментов времени, в которые данные воздействия проводятся. При этом учитывались различные характеристики (показатели) объекта исследования (табл. 1).

Для математической оценки степени уязвимости факторов применен коэффициент структурной угрозы  $K_c$  [6], представляющий собой количественное соотношение пораженных импульсом узлов к общему количеству узлов системы

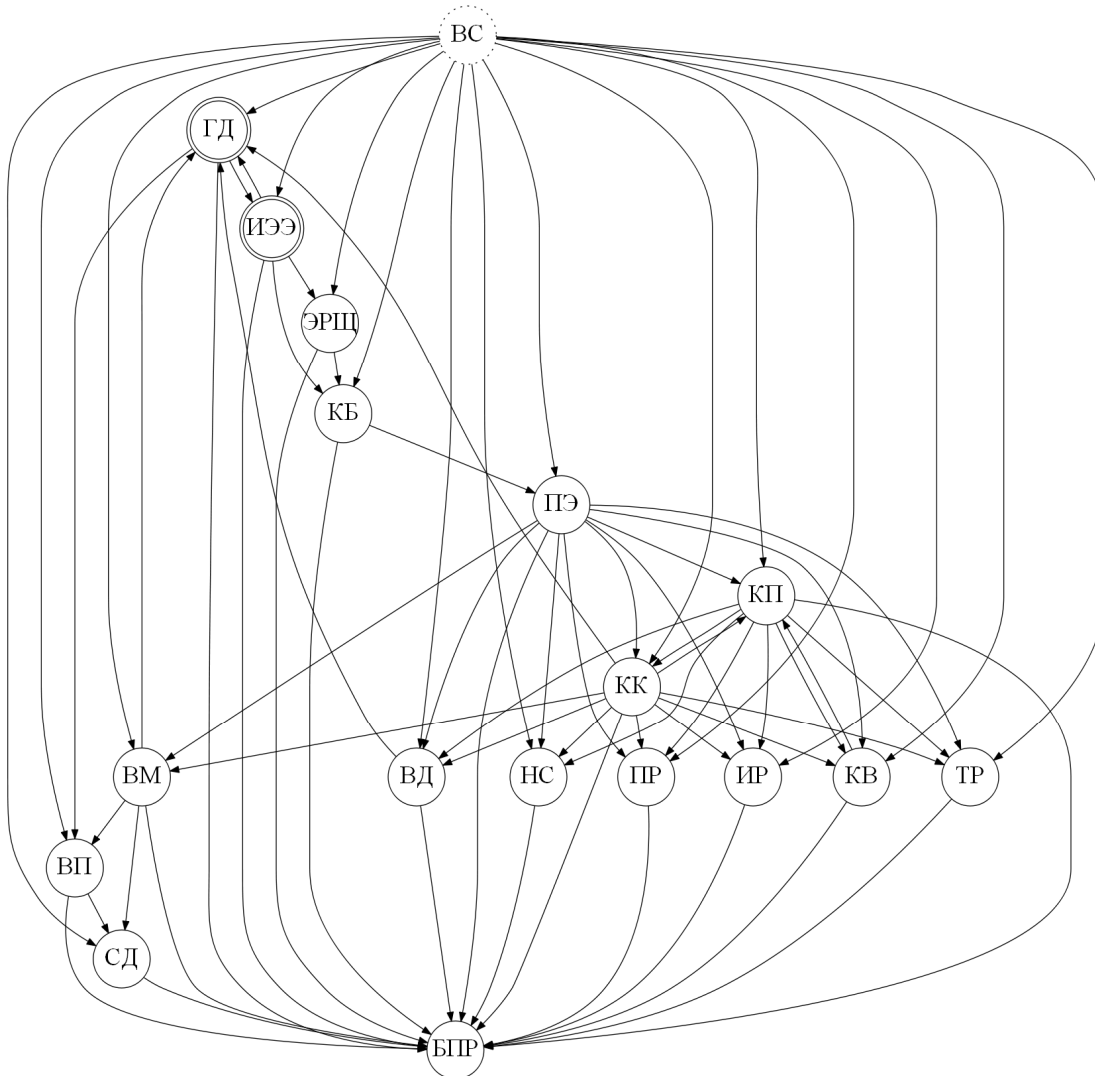
$$K_c(F_i) = \frac{i}{N},$$

где

$F_i$  — объект системы, на который воздействует единичный поражающий импульс;

$i$  — общее количество пораженных объектов;

$N$  — общее количество объектов в системе.



**Рис. 4.** Когнитивная карта взаимозависимости и взаимосвязанности СКТС

Установленные в ходе исследований и расчетов значения коэффициента структурной уязвимости по агрегатам СКТС приведены на гистограмме рис. 5. На оси абсцисс показаны наименования всех объектов полученной информационной когнитивной модели, на оси ординат – диапазон значений, которые принимает коэффициент структурной уязвимости (от 0 до 1 с шагом 0,1).



Таблица 1.

Характеристики показателей модели

| №  | Название объекта                 | Блок объекта | Оценка         |
|----|----------------------------------|--------------|----------------|
| 1  | Главный двигатель                | СЭУ          | Качественная   |
| 2  | Судовой движитель                | СЭУ          | Качественная   |
| 3  | Валопровод                       | СЭУ          | Качественная   |
| 4  | Вспомогательные механизмы        | СЭУ          | Качественная   |
| 5  | Источники электроэнергии         | СЭС          | Количественная |
| 6  | Линии электропередач             | СЭС          | Качественная   |
| 7  | Электрораспределительные щиты    | СЭС          | Качественная   |
| 8  | Преобразователи электроэнергии   | СЭС          | Количественная |
| 9  | Трюмные системы                  | СВС          | Качественная   |
| 10 | Системы наливных судов           | СВС          | Качественная   |
| 11 | Измерительные системы            | СВС          | Качественная   |
| 12 | Переговорные системы             | СВС          | Качественная   |
| 13 | Воздушные системы                | СВС          | Качественная   |
| 14 | Комплекс пожаротушения           | СВС          | Качественная   |
| 15 | Комплекс водоснабжения           | СВС          | Количественная |
| 16 | Климатический комплекс           | СВС          | Количественная |
| 17 | Морское волнение                 | ВС           | Качественная   |
| 18 | Воздействие ветра                | ВС           | Качественная   |
| 19 | Воздействие подвижных объектов   | ВС           | Качественная   |
| 20 | Воздействие неподвижных объектов | ВС           | Качественная   |
| 21 | Штормовое воздействие            | ВС           | Качественная   |

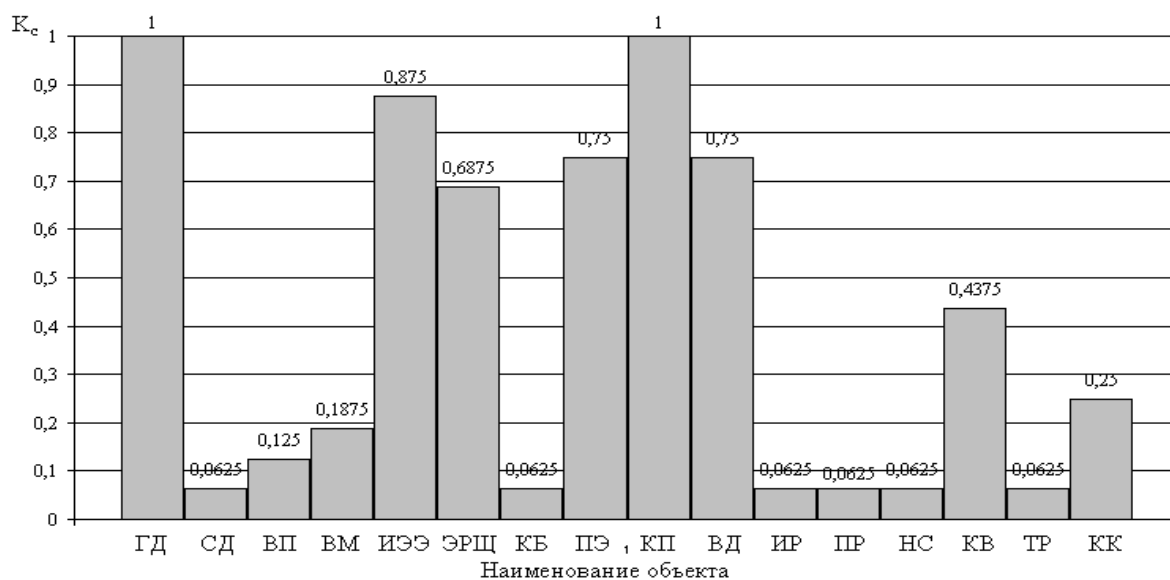


Рис. 5. Значения коэффициентов структурной уязвимости по агрегатам СКТС

Из результатов проведенных исследований следует, что наиболее уязвимыми в СКТС являются главный двигатель (СЭУ), комплекс пожаротушения (СВС), источники электроэнергии (СЭС), что связано с высокой степенью их зависимости от других агрегатов СКТС.

Полученные результаты информационно когнитивного моделирования взаимозависимых и взаимосвязанных СТС позволяют описать механизм их функционирования, сценарии возможного развития, структурные свойства. Разработанная информационная когнитивная модель СКТС является основой проектируемой системы поддержки принятия решений при оценке и обеспечении надежности функционирования СТС.

## Выводы

Полученные результаты исследования информационной когнитивной модели взаимозависимых и взаимосвязанных СКТС показали работоспособность модели, а также целесообразность применения метода когнитивного моделирования для исследования сложных технических систем. Использование предложенного метода расчета значений коэффициентов структурной уязвимости обеспечивает определение наиболее уязвимых и критичных по надежности агрегатов СКТС. Полученные результаты исследований и разработок позволяют повысить эффективность эксплуатации сложных технических систем, обеспечить качественное прогнозирование надежности их функционирования в аварийных экстремальных ситуациях.

Использование информационных когнитивных моделей сложных технических систем является первоочередным этапом при проектировании систем поддержки принятия решений, что позволит автоматизировать и оптимизировать процесс оценки надежности сложных технических систем.

## Список литературы

1. Максимов, В.И. Развитие моделей принятия решений: проблемы, парадоксы и перспективы / В.И. Максимов // *Банковские технологии*. — 2000. — № 3. — С. 39–43.
2. Максимов, В.И. Анализ и управление в нестабильной среде / В.И. Максимов, С.В. Качаев, Е.К. Корноушенко // *Банковские технологии*. — 1999. — № 3. — С. 47–52.
3. Максимов, В.И. Когнитивный анализ и моделирование сложных ситуаций / В.И. Максимов, Е.К. Корноушенко, С.В. Качаев // *Банковские технологии*. — 2001. — № 7. — С. 21–26.
4. Шередеко, Ю.Л. Классификация информационных процессов. Когнитивные процессы / Ю.Л. Шередеко // *Управляющие системы и машины УС и М*. — 1998. — № 1. — С. 5–17.
5. Горелова, Г.В. Когнитивное моделирование для интеллектуальной системы поддержки принятия решений управления транзитной торговлей / Г.В. Горелова, А.И. Хлебникова // *Искусственный интеллект*. — 2010. — № 3. — С. 473–482.
6. Бойко, В.Д. Модель оценки живучести судовых технических систем / В.Д. Бойко, В.В. Вычужанин // *Вестник НУК*. — 2012. — № 3. — С. 62–67.

**ІНФОРМАЦІЙНА КОГНІТИВНА МОДЕЛЬ ТЕХНОЛОГІЧНОЇ ВЗАЄМОЗАЛЕЖНОСТІ СУДНОВИХ ТЕХНІЧНИХ ЗАСОБІВ**

Н.Д. Рудніченко, В.В. Вичужанін

Одеський національний морський університет,  
вул. Мечникова, 34, Одеса, 65404, Україна; e-mail: rudnick@mail.ua

У статті наведено результати досліджень розробленої інформаційної когнітивної моделі технологічної взаємозалежності і взаємозв'язку складних технічних систем для оцінки їх вразливості. Побудовано загальну структурну схему взаємопов'язаності суднових складних технічних систем. Досліджено взаємодію агрегатів суднової енергетичної установки, системи енергопостачання судна і суднових допоміжних систем в аварійних екстремальних ситуаціях. На підставі отриманих результатів досліджень розроблено інформаційну когнітивну модель технологічної взаємозалежності функціонування суднових складних технічних систем. Відповідно до створеним алгоритмом оцінки вразливості елементів інформаційної когнітивної моделі зроблено розрахунок коефіцієнтів структурної уразливості її елементів. Результати розрахунку дозволили визначити найбільш критичні за надійності елементи моделі. Отримані результати досліджень і розробок дозволяють підвищити ефективність експлуатації складних технічних систем, забезпечити якісне прогнозування надійності їх функціонування в аварійних екстремальних ситуаціях.

**Ключові слова:** взаємозалежність, взаємозв'язок, когнітивне моделювання, надійність, система підтримки та прийняття рішень

**INFORMATION COGNITIVE MODEL OF TECHNOLOGICAL INTERDEPENDENCE OF MARINE TECHNICAL RECOURSES**

Nick D. Rudnichenko, Vladimir V. Vichuzhanin

Odessa National Maritime University,  
34 Mechnikova str., Odessa, 65404, Ukraine; e-mail: rudnick@mail.ua

This paper contains the results of studies of the cognitive model developed information technology interdependence and interrelation of complex technical systems to assess their vulnerability. A general block diagram of a ship interconnectedness of complex technical systems. The interaction of ship power plant units, the power supply system of the ship and ship's auxiliary systems in extreme emergency situations. Based on the results of research developed an information processing model of cognitive functioning marine interdependence of complex technical systems. In accordance with the established algorithm vulnerability assessment information elements of the cognitive model calculated the coefficients of the structural vulnerability of its elements. The calculation results have allowed to identify the most critical elements of the model in terms of reliability. The results of research and development will improve the efficiency of operation of complex technical systems that provide high-quality prediction of the reliability of their operation in extreme emergency situations.

**Keywords:** interdependence, interaction, cognitive modeling, reliability, support system and decision-making

# ПОВЫШЕНИЕ СКРЫТОЙ ПРОПУСКНОЙ СПОСОБНОСТИ УСТОЙЧИВЫХ К СЖАТИЮ СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМОВ ДЛЯ ПРОИЗВОЛЬНЫХ ИЗОБРАЖЕНИЙ-КОНТЕЙНЕРОВ

М.А. Мельник

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

Разработан стеганографический алгоритм, устойчивый к атаке сжатием, в том числе, с малыми коэффициентами качества. В качестве контейнера используется цифровое изображение, хранимое в произвольном формате. Разработка алгоритма проведена на основе существующих аналогов, математическим базисом которых является общий подход к анализу состояния и технологии функционирования информационных систем. Основным преимуществом нового стеганоалгоритма является увеличение в 6 раз его скрытой пропускной способности, по сравнению с алгоритмами, положенными в его основу. Приведены результаты вычислительного эксперимента, подтверждающие высокую эффективность декодирования погруженной информации в условиях атаки сжатием с малыми коэффициентами качества на стеганосообщение.

**Ключевые слова:** стеганографический алгоритм, атака сжатием, стеганосообщение, цифровое изображение, симметричная матрица, собственные значения, собственные векторы, спектральное разложение

## Введение

Задача разработки стеганографических алгоритмов, устойчивых к распространенной на сегодняшний день атаке сжатием, относящейся к атакам против встроенного сообщения, направленной на разрушение дополнительной информации, является актуальной и нерешенной до конца [1]. Решению этой задачи посвящено много современных научных изысканий, в том числе, [2–4], где автором настоящей работы на базе общего подхода к анализу состояния и технологии функционирования информационных систем [5, 6] были предложены стеганоалгоритмы, использующие в качестве контейнера, или основного сообщения (ОС), цифровые изображения (ЦИ), хранящиеся в произвольном формате, обозначаемые далее  $A_1$ ,  $A_2$ ,  $A_3$ , устойчивые к атаке сжатием, значительно превосходящие свои современные аналоги ( $S_1$  [7],  $S_2$  [8],  $S_3$  [9],  $S_4$  [10],  $S_5$  [11],  $S_6$  [12],  $S_7$  [13],  $S_8$  [14],  $S_9$  [15],  $S_{10}$  [16],  $S_{11}$  [17],  $SS_1$ ,  $SS_2$  [18]) по эффективности декодирования в условиях сжатия со значительными коэффициентами (табл. 1). В [2–4] и настоящей работе атака сжатием на стеганосообщение (СС), являющееся результатом стеганообразования, моделируется путем пересохранения СС в формат Jpeg с различными коэффициентами качества  $QF$  в общедоступном графическом редакторе IrfanView, эффективность стеганоалгоритма оценивается стандартным образом: при помощи коэффициента корреляции  $NC$  для дополнительной информации (ДИ), в качестве которой выступает случайно сформированная бинарная последовательность:  $NC = \frac{1}{t} \sum_{i=1}^t p_i \times \bar{p}_i$ , где  $p_1, p_2, \dots, p_t$ ;

$\bar{p}_1, \bar{p}_2, \dots, \bar{p}_t, p_i, \bar{p}_i \in \{0,1\}, i = \bar{1}, t$ , — соответственно погруженная и декодированная из стеганосообщения ДИ;  $p_i' = 1, \bar{p}_i' = 1$ , если  $p_i = 1, \bar{p}_i = 1$ , и  $p_i' = -1, \bar{p}_i' = -1$ , если  $p_i = 0, \bar{p}_i = 0$ , т.е.  $p_i' \times \bar{p}_i' \in \{1, -1\}$ .

Один из разработанных алгоритмов (A1) [2] основан на возмущениях максимальных сингулярных чисел (СНЧ) блоков матрицы контейнера, полученных после ее стандартного разбиения, другой (A2) – на sign-нечувствительности левых и правых сингулярных векторов (СНВ) блоков, соответствующих максимальным СНЧ [3], третий (A3), являясь комбинацией A1 и A2 [4], позволил повысить скрытую пропускную способность (СПС) [1] базовых стеганоалгоритмов, составляющую 1/64 бит/пиксель, в три раза. Однако СПС 3/64 бит/пиксель, достигнутая в A3, оставляет желание и возможность ее повышения.

**Таблица 1.**

Значение *NC* для различных стеганоалгоритмов при атаке сжатием с различными коэффициентами качества на стеганосообщение

| Стегано-алгоритм       | <i>QF</i> |      |       |      |       |       |      |      |      |      |      |
|------------------------|-----------|------|-------|------|-------|-------|------|------|------|------|------|
|                        | 10        | 20   | 25    | 30   | 40    | 50    | 60   | 70   | 75   | 80   | 90   |
| <i>S</i> <sub>1</sub>  | -         | -    | -     | 0.15 | -     | 0.28  | -    | 0.57 | -    | -    | 1    |
| <i>S</i> <sub>2</sub>  | 0.15      | 0.34 | -     | 0.52 | -     | 0.52  | -    | 0.63 | -    | -    | 0.80 |
| <i>S</i> <sub>3</sub>  | 0.17      | 0.61 | -     | 0.79 | -     | 0.89  | -    | 0.97 | -    | -    | 1    |
| <i>S</i> <sub>4</sub>  | 0.34      | 0.67 | -     | 0.82 | -     | 0.96  | -    | 0.97 | -    | -    | 0.99 |
| <i>S</i> <sub>5</sub>  | -         | -    | 0.63  | -    | 0.80  | 0.89  | -    | -    | -    | -    | -    |
| <i>S</i> <sub>6</sub>  | -         | -    | 0.801 | -    | 0.828 | 0.916 | -    | -    | -    | -    | -    |
| <i>S</i> <sub>7</sub>  | -         | -    | -     | -    | -     | -     | 0.70 | 0.95 | -    | 0.99 | 0.99 |
| <i>S</i> <sub>8</sub>  | -         | 0.85 | -     | -    | -     | 0.87  | -    | -    | -    | 0.90 | -    |
| <i>S</i> <sub>9</sub>  | -         | 0.84 | -     | -    | -     | 0.93  | -    | -    | -    | 0.97 | -    |
| <i>S</i> <sub>10</sub> | 0.86      | 0.95 | -     | 0.95 | 0.97  | 0.98  | 0.98 | 0.98 | -    | 0.98 | 0.99 |
| <i>S</i> <sub>11</sub> | 0.42      | 0.56 | -     | 0.80 | 0.95  | 0.95  | 1    | 1    | -    | 1    | 1    |
| <i>SS</i> <sub>1</sub> | -         | -    | 0.67  | -    | -     | 0.80  | -    | -    | 0.92 | -    | -    |
| <i>SS</i> <sub>2</sub> | -         | -    | 0.7   | -    | -     | 0.91  | -    | -    | 0.95 | -    | -    |
| <i>A1</i>              | 0.87      | 0.93 | 0.94  | 0.95 | 0.96  | 0.98  | 0.98 | 0.98 | 0.98 | 0.98 | 0.98 |
| <i>A2</i>              | 0.94      | 0.95 | 0.95  | 0.95 | 0.95  | 0.95  | 0.95 | 0.96 | 0.96 | 0.96 | 0.96 |
| <i>A3</i>              | 0.90      | 0.93 | 0.93  | 0.93 | 0.93  | 0.94  | 0.94 | 0.94 | 0.94 | 0.94 | 0.94 |

**Цель статьи и постановка исследований**

Целью настоящей работы является разработка полиномиального стеганоалгоритма, устойчивого к атаке сжатием, в том числе при малых коэффициентах качества, на основе алгоритмов, предложенных автором ранее (A1, A2, A3), для повышения СПС организуемого скрытого канала связи, по сравнению с СПС для A1, A2, A3.

Для достижения поставленной цели в работе решаются следующие задачи:

- 1) Увеличения СПС канала скрытой связи за счет виртуальной симметризации матриц блоков ЦИ-контейнера;
- 2) Оценка вычислительной сложности разработанного стеганоалгоритма.

3) Сравнительная оценка эффективности декодирования ДИ разработанным стеганоалгоритмом в условиях атаки сжатием на стеганосообщение.

**Основная часть**

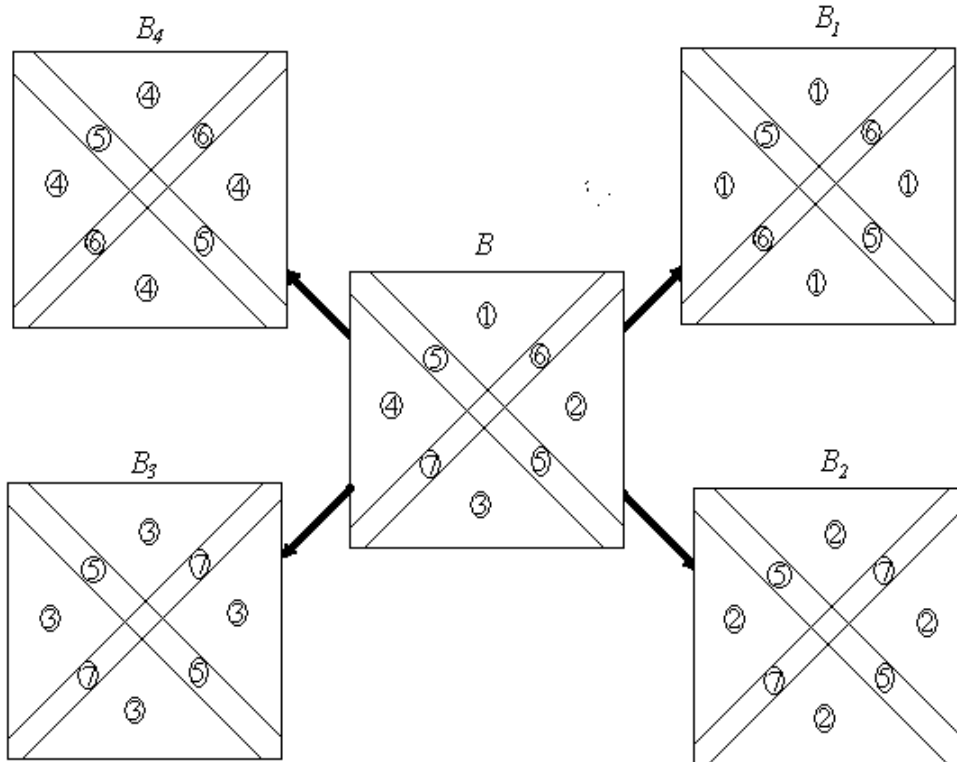
Пусть  $F$  —  $m \times n$ -матрица ЦИ-контейнера. В качестве ДИ рассматривается случайно сформированная бинарная последовательность  $p_1, \dots, p_t, p_i \in \{0,1\}, i = \overline{1,t}$ . Пусть  $B$  — произвольный  $8 \times 8$ -блок матрицы ОС, полученный после ее стандартного разбиения [19]. Матрице  $B$  поставим в соответствии четыре симметричные матрицы  $B_1, B_2, B_3, B_4$  по правилу, называемому далее правилом  $SB$ , наглядно представленному на рис. 1 (здесь цифрами 5,6,7 обозначены главная и части побочной диагонали  $B$ ), отражая относительно главной и побочной диагоналей треугольные части, обозначенные цифрами 1,2,3,4, исходной матрицы соответственно, которые и будем рассматривать ниже как блоки контейнера. Для каждого из полученных виртуальных блоков в силу их симметричности возможно построение нормального спектрального разложения [20]:

$$B_i = U_i \Lambda_i U_i^T, \quad i = \overline{1,4}, \tag{1}$$

где

$U_i, i = \overline{1,4}$ , — матрицы ортонормированных лексикографически положительных собственных векторов (СВ),

$\Lambda_i = \text{diag}(\lambda_1^{(i)}, \dots, \lambda_8^{(i)})$ ,  $i = \overline{1,4}$ , — матрицы собственных значений (СЗ)  $B_i, i = \overline{1,4}$ , соответственно.



**Рис. 1.** Правило  $SB$  получения симметричных виртуальных блоков матрицы контейнера

По аналогії с АЗ [4], обозначим  $K$  – пороговое значение вариации возмущений максимальных СЗ блоков (в соответствии с [2], учитывая связь между СНЧ и СЗ симметричной матрицы [20],  $K$  берется равным 200 для СЗ, как и для СНЧ несимметричных блоков в СА А1),  $n^o = \left( \frac{1}{\sqrt{8}}, \dots, \frac{1}{\sqrt{8}} \right)^T \in R^8$  —  $n$ -оптимальный вектор пространства  $R^8$ , обладающий максимальной sign-устойчивостью к произвольным возмущающим воздействиям [6].

Основные шаги предлагаемого стеганоалгоритма, называемого далее А4, следующие.

**Погружение ДИ.**

Шаг 1. Матрица  $F$  контейнера разбивается стандартным образом на блоки  $B$  размером  $8 \times 8$ . Каждый блок используется для погружения 6 бит ДИ.

Шаг 2. (Погружение ДИ). Пусть  $B$  — очередной блок с элементами  $b_{ml}$ ,  $m, l = \overline{1,8}$ , используемый для стеганопреобразования.

2.1. Каждому блоку  $B$  ставятся в соответствии симметричные блоки  $B_i$ ,  $i = \overline{1,4}$ , по правилу  $SB$ ;  $p_i, p_{i+1}, \dots, p_{i+5}$  — очередные 6 бит ДИ.

2.2. Строятся нормальные спектральные разложения (1) для  $B_i$ ,  $i = \overline{1,4}$ .

2.3.

Если  $p_i = 0$ ,

то  $\bar{\lambda}_1^{(1)} = \lambda_2^{(1)} + K \left( n + \frac{1}{4} \right)$ ,

где  $n$  — натуральное число здесь и ниже;

иначе  $\bar{\lambda}_1^{(1)} = \lambda_2^{(1)} + K \left( n + \frac{3}{4} \right)$ .

2.4.

Если  $p_{i+1} = 0$ ,

то  $\bar{\lambda}_1^{(2)} = \lambda_2^{(2)} + K \left( n + \frac{1}{4} \right)$ ,

иначе  $\bar{\lambda}_1^{(2)} = \lambda_2^{(2)} + K \left( n + \frac{3}{4} \right)$ .

2.5.

Если  $p_{i+2} = 1$ ,

то 2.5.1  $\bar{u}_1^{(1)} = n^o$ ,

где  $\bar{u}_1^{(1)}$  — возмущенный в ходе СП  $u_1^{(1)}$ ;

2.5.2 Приведение СВ  $u_2^{(1)}, \dots, u_8^{(1)}$  блока  $B_1$  к ортонормированному с  $\bar{u}_1^{(1)}$  лексикографически положительному виду. Результат —  $\bar{u}_2^{(1)}, \dots, \bar{u}_8^{(1)}$ .

иначе 2.5.1  $\bar{u}_1^{(2)} = n^o$ ,

где  $\bar{u}_1^{(2)}$  — возмущенный в ходе СП  $u_1^{(2)}$ ;

2.5.2 Приведение СВ  $u_2^{(2)}, \dots, u_8^{(2)}$  блока  $B_2$  к ортонормированному с  $\bar{u}_1^{(2)}$  лексикографически положительному виду. Результат —  $\bar{u}_2^{(2)}, \dots, \bar{u}_8^{(2)}$ .

2.6.

Если  $p_{i+3} = 0$ ,

то  $\bar{\lambda}_1^{(3)} = \lambda_2^{(3)} + K \left( n + \frac{1}{4} \right);$

иначе  $\bar{\lambda}_1^{(3)} = \lambda_2^{(3)} + K \left( n + \frac{3}{4} \right).$

2.7.

Если  $p_{i+4} = 0,$

то  $\bar{\lambda}_1^{(4)} = \lambda_2^{(4)} + K \left( n + \frac{1}{4} \right);$

иначе  $\bar{\lambda}_1^{(4)} = \lambda_2^{(4)} + K \left( n + \frac{3}{4} \right).$

2.8.

Если  $p_{i+5} = 1,$

то 2.8.1  $\bar{u}_1^{(3)} = n^o,$

где  $\bar{u}_1^{(3)}$  — возмущенный в ходе СП  $u_1^{(3)}$ ;

2.8.2 Приведение СВ  $u_2^{(3)}, \dots, u_8^{(3)}$  блока  $B_3$  к ортонормированному с  $\bar{u}_1^{(3)}$  лексикографически положительному виду. Результат —  $\bar{u}_2^{(3)}, \dots, \bar{u}_8^{(3)}$ .

иначе 2.8.1  $\bar{u}_1^{(4)} = n^o,$

где  $\bar{u}_1^{(4)}$  — возмущенный в ходе СП  $u_1^{(4)}$ ;

2.8.2 Приведение СВ  $u_2^{(4)}, \dots, u_8^{(4)}$  блока  $B_2$  к ортонормированному с  $\bar{u}_1^{(2)}$  лексикографически положительному виду. Результат —  $\bar{u}_2^{(4)}, \dots, \bar{u}_8^{(4)}$ .

Шаг 3. Формирование блока СС.

3.1.

Если  $p_{i+2} = 1,$

то  $\bar{B}_1 = \bar{U}_1 \bar{\Lambda}_1 \bar{U}_1^T, \bar{B}_2 = U_2 \bar{\Lambda}_2 U_2^T,$

где  $\bar{U}_1 = (n^o, \bar{u}_2^{(1)}, \dots, \bar{u}_8^{(1)}), \bar{\Lambda}_1 = \text{diag}(\bar{\lambda}_1^{(1)}, \dots, \lambda_8^{(1)}),$

$\bar{\Lambda}_2 = \text{diag}(\bar{\lambda}_1^{(2)}, \dots, \lambda_8^{(2)});$

иначе  $\bar{B}_1 = U_1 \bar{\Lambda}_1 U_1^T, \bar{B}_2 = \bar{U}_2 \bar{\Lambda}_2 \bar{U}_2^T,$

где  $\bar{U}_2 = (n^o, \bar{u}_2^{(2)}, \dots, \bar{u}_8^{(2)}), \bar{\Lambda}_1 = \text{diag}(\bar{\lambda}_1^{(1)}, \lambda_2^{(1)}, \dots, \lambda_8^{(1)}),$

$\bar{\Lambda}_2 = \text{diag}(\bar{\lambda}_1^{(2)}, \lambda_2^{(2)}, \dots, \lambda_8^{(2)}).$

3.2.

Если  $p_{i+5} = 1,$

то  $\bar{B}_3 = \bar{U}_3 \bar{\Lambda}_3 \bar{U}_3^T, \bar{B}_4 = U_4 \bar{\Lambda}_4 U_4^T,$

где  $\bar{U}_3 = (n^o, \bar{u}_2^{(3)}, \dots, \bar{u}_8^{(3)}), \bar{\Lambda}_3 = \text{diag}(\bar{\lambda}_1^{(3)}, \dots, \lambda_8^{(3)}),$

$\bar{\Lambda}_4 = \text{diag}(\bar{\lambda}_1^{(4)}, \dots, \lambda_8^{(4)});$

иначе  $\bar{B}_3 = U_3 \bar{\Lambda}_3 U_3^T, \bar{B}_4 = \bar{U}_4 \bar{\Lambda}_4 \bar{U}_4^T,$

где  $\bar{U}_4 = (n^o, \bar{u}_2^{(4)}, \dots, \bar{u}_8^{(4)}), \bar{\Lambda}_3 = \text{diag}(\bar{\lambda}_1^{(3)}, \dots, \lambda_8^{(3)}),$

$\bar{\Lambda}_4 = \text{diag}(\bar{\lambda}_1^{(4)}, \dots, \lambda_8^{(4)}).$

3.3. Элементы матриц  $\bar{B}_i, i = 1, 2, 3, 4,$  обозначим соответственно  $\bar{b}_{ml}^{(i)}, m, l = \bar{1}, \bar{8}.$

Блок  $\bar{B}$  СС будет иметь вид:



$$\bar{B} = \begin{pmatrix} b_{11} & \bar{b}_{12}^{(1)} & \bar{b}_{13}^{(1)} & \bar{b}_{14}^{(1)} & \bar{b}_{15}^{(1)} & \bar{b}_{16}^{(1)} & \bar{b}_{17}^{(1)} & b_{18} \\ \bar{b}_{21}^{(4)} & b_{22} & \bar{b}_{23}^{(1)} & \bar{b}_{24}^{(1)} & \bar{b}_{25}^{(1)} & \bar{b}_{26}^{(1)} & b_{27} & \bar{b}_{28}^{(2)} \\ \bar{b}_{31}^{(4)} & \bar{b}_{32}^{(4)} & b_{33} & \bar{b}_{34}^{(1)} & \bar{b}_{35}^{(1)} & b_{36} & \bar{b}_{37} & \bar{b}_{38}^{(2)} \\ \bar{b}_{41}^{(4)} & \bar{b}_{42}^{(4)} & \bar{b}_{43}^{(4)} & b_{44} & b_{45} & \bar{b}_{46}^{(2)} & \bar{b}_{47}^{(2)} & \bar{b}_{48}^{(2)} \\ \bar{b}_{51}^{(4)} & \bar{b}_{52}^{(4)} & \bar{b}_{53}^{(4)} & b_{54} & b_{55} & \bar{b}_{56}^{(2)} & \bar{b}_{57}^{(2)} & \bar{b}_{58}^{(2)} \\ \bar{b}_{61}^{(4)} & \bar{b}_{62}^{(4)} & b_{63} & \bar{b}_{64}^{(3)} & \bar{b}_{65}^{(3)} & b_{66} & \bar{b}_{67}^{(2)} & \bar{b}_{68}^{(2)} \\ \bar{b}_{71}^{(4)} & b_{72} & \bar{b}_{73}^{(3)} & \bar{b}_{74}^{(3)} & \bar{b}_{75}^{(3)} & \bar{b}_{76}^{(3)} & b_{77} & \bar{b}_{78}^{(2)} \\ b_{81} & \bar{b}_{82}^{(3)} & \bar{b}_{83}^{(3)} & \bar{b}_{84}^{(3)} & \bar{b}_{85}^{(3)} & \bar{b}_{86}^{(3)} & \bar{b}_{87}^{(3)} & b_{88} \end{pmatrix}. \quad (2)$$

**Декодирование ДИ.**

Шаг 1. Матрица  $\bar{F}$  СС разбивается стандартным образом на блоки  $\bar{B}$  размером  $8 \times 8$ . Каждый блок используется для декодирования 6 бит ДИ.

Шаг 2. (Декодирование ДИ). Пусть  $\bar{B}$  — очередной блок, из которого извлекаются биты  $\bar{p}_i, \bar{p}_{i+1}, \dots, \bar{p}_{i+5}$  ДИ.

2.1. Каждому блоку  $\bar{B}$  ставятся в соответствии симметричные блоки  $\bar{B}_i$ ,  $i = \overline{1,4}$ , в соответствии с правилом  $SB$ .

2.2. Строятся нормальные спектральные разложения вида (1).

$$\bar{B}_i = \bar{U}_i \bar{\Lambda}_i \bar{U}_i^T, \quad i = \overline{1,4}.$$

2.3.

Если

$$\text{mod}([\bar{\lambda}_1^{(1)} - \bar{\lambda}_2^{(1)}], K) < \frac{K}{2},$$

где  $[\bullet]$  — целая часть аргумента;

то

$$\bar{p}_i = 0;$$

иначе

$$\bar{p}_i = 1.$$

2.4.

Если

$$\text{mod}([\bar{\lambda}_1^{(2)} - \bar{\lambda}_2^{(2)}], K) < \frac{K}{2};$$

то

$$\bar{p}_{i+1} = 0;$$

иначе

$$\bar{p}_{i+1} = 1.$$

2.5. Найти  $UN_1$  и  $UN_1$  — углы между векторами  $\bar{u}_1^{(1)}$  и  $n^o$ ,  $\bar{u}_1^{(2)}$  и  $n^o$  соответственно.

Если

$$UN_1 < UN_2;$$

то

$$\bar{p}_{i+2} = 1;$$

иначе

$$\bar{p}_{i+2} = 0.$$

2.6.

Если

$$\text{mod}([\bar{\lambda}_1^{(3)} - \bar{\lambda}_2^{(3)}], K) < \frac{K}{2};$$

то  $\bar{p}_{i+3} = 0;$

иначе  $\bar{p}_{i+3} = 1.$

2.7.

Если  $\text{mod}([\bar{\lambda}_1^{(4)} - \bar{\lambda}_2^{(4)}]K) < \frac{K}{2};$

то  $\bar{p}_{i+4} = 0;$

иначе  $\bar{p}_{i+4} = 1.$

2.8. Найти  $UN_3$  и  $UN_4$  - углы между векторами  $\bar{u}_1^{(3)}$  и  $n^o$ ,  $\bar{u}_1^{(4)}$  и  $n^o$  соответственно.

Если  $UN_3 < UN_4;$

то  $\bar{p}_{i+5} = 1;$

иначе  $\bar{p}_{i+5} = 0.$

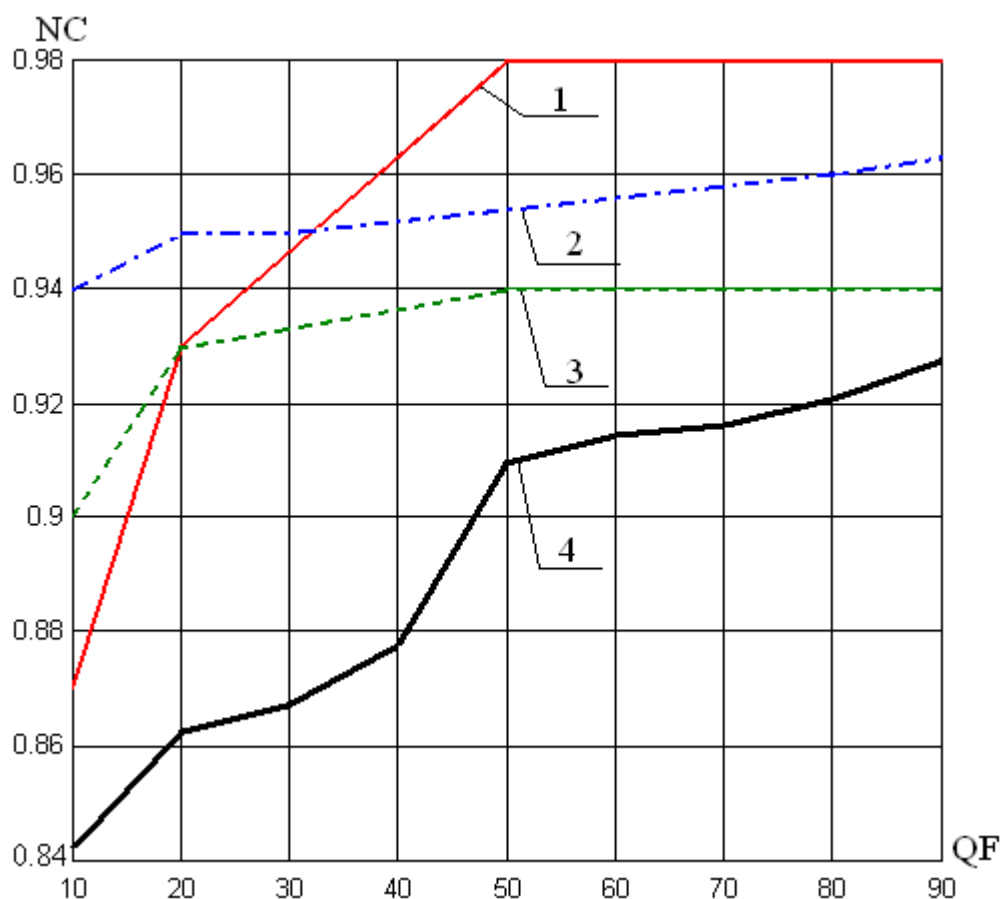
**Замечание 1.** Вычислительная сложность разработанного стеганоалгоритма  $A4$  определяется количеством блоков матрицы  $F$  ЦИ-контейнера, получаемых в результате ее стандартного разбиения, и в случае, когда матрица имеет размеры  $n \times n$  пикселей, будет оцениваться как  $O(n^2)$  операций.

**Замечание 2.** В алгоритме  $A4$  в качестве виртуальных блоков матрицы контейнера используются симметричные блоки. Это требование не является обязательным, т.е. матрице блока  $B$  не обязательно ставить в соответствие блоки  $B_1, B_2, B_3, B_4$  по правилу, отраженному на рис. 1. Однако, основной вычислительный шаг при обработке каждого блока контейнера в  $A4$  – это построение спектрального разложения, которое, в случае несимметричности блоков  $B_1, B_2, B_3, B_4$  целесообразно будет заменить на сингулярное разложение, что, как известно, потребует больше вычислительных затрат для своей реализации [20], а потому является нежелательным.

**Замечание 3.** Учитывая вид (2) блока  $CC$ , а именно предложенный способ построения главной и побочной диагоналей (они остаются неизменными по сравнению с диагоналями контейнера), очевидным является увеличение вычислительной погрешности при формировании  $CC$  в  $A4$  по сравнению с  $A1, A2, A3$ , и предсказуемое ухудшение эффективности. Такой результат является своеобразной «платой» за увеличение СПС соответствующего скрытого канала связи по сравнению с аналогичным параметром для  $A1, A2, A3$ .

Результаты сравнения эффективностей декодирования ДИ стеганоалгоритмов  $A1, A2, A3, A4$  в условиях атаки сжатием на  $CC$  с различными коэффициентами качества для контейнеров в формате TIF представлены на рис. 2.

Из результатов эксперимента видно, что эффективность  $A4$  действительно несколько уступает алгоритмам  $A1, A2, A3$ , но остается достаточно высокой по сравнению с другими современными аналогами, использованными для сравнения (табл. 1), особенно при малых  $QF$ . При этом разработанный стеганоалгоритм  $A4$  имеет скрытую пропускную способность, превосходящую СПС  $A1, A2$  в 6 раз,  $A3$  – в два раза, и составляет 3/32 бит/пиксель.



**Рис. 2.** Ефективність декодування ДІ розробленими стеганоалгоритмами: 1 –  $A1$ ; 2 –  $A2$ ; 3 –  $A3$ ; 4 –  $A4$

### Заключення

В настоящей работе разработан стеганографический алгоритм  $A4$ , устойчивый к сжатию со значительными коэффициентами: так для  $QF=10$  среднее значение  $NC > 0.84$ , при этом скрытая пропускная способность канала связи, организуемого при помощи  $A4$ , составила  $3/32$  бит/пиксель, что в 6 раза превысило СПС  $A1$ ,  $A2$ , положенных в его основу. Вычислительная сложность алгоритма составила  $\underline{O}(n^2)$  операций.

Основным возмущающим воздействием для получаемого при помощи  $A4$  стеганосообщения, очевидно является процесс округлений, происходящий после СП. Это заключение определяет направление дальнейших исследований автора: организации процесса СП таким образом, чтобы уменьшить вычислительную погрешность при построении СС.

### Список литературы

1. Стеганография, цифровые водяные знаки и стеганоанализ : [монография] / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. — М.: Вузовская книга, 2009. — 220 с.
2. Мельник, М.А. Стеганоалгоритм, устойчивый к сжатию / М.А. Мельник // Інформаційна безпека. — 2012. — № 2(8). — С. 99–106.

3. Мельник, М.А. Sign-нечувствительность сингулярных векторов матрицы изображения как основа стеганоалгоритма, устойчивого к сжатию / М.А. Мельник // Информатика та математичні методи в моделюванні. — 2013. — Том 3, № 2. — С. 146–155.
4. Мельник, М.А. Повышение скрытой пропускной способности стеганографических алгоритмов, устойчивых к атаке сжатием / М.А. Мельник // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. — 2013. — Вип. 41. — С. 56–62.
5. Кобозева, А.А. Формальные условия обеспечения устойчивости стеганометода к сжатию / А.А. Кобозева, М.А. Мельник // Сучасна спеціальна техніка. — 2012. — № 4(31). — С. 60–69.
6. Кобозева, А.А. Нечувствительность стеганосообщения к сжатию и формальные достаточные условия ее обеспечения / А.А. Кобозева, М.А. Мельник // Збірник наукових праць Військового інституту Київського нац-го ун-ту ім. Т.Шевченка. — 2012. — Вип. 38. — С. 193–203.
7. Wang, S.H. Wavelet tree quantization for copyright protection watermarking / S.H. Wang, Y.P. Lin // IEEE Transactions on Image Processing. — 2004. — Vol. 13, Iss. 2. — PP. 154–165.
8. Li, E. An integer wavelet based multiple logo-watermarking scheme / E. Li, H. Liang, X. Niu // Proceedings of the IEEE WCICA. — 2006. — PP.10256–10260.
9. Lien, B.K. A watermarking method based on maximum distance wavelet tree quantization / B.K. Lien, W.H. Lin // Proceedings of the 19<sup>th</sup> Conference on Computer Vision, Graphics and Image Processing. — 2006. — PP. 269–276.
10. Lin, W.-H. A blind watermarking method using maximum wavelet coefficient quantization / W.-H. Lin *et al.* // Expert Systems with Applications. — 2009. — Vol. 36, Iss. 9. — PP. 11509–11516.
11. Li, C. A novel watermarking scheme for image authentication in DWT domain / C. Li, H. Song // Proceedings of 3<sup>rd</sup> International Conference on Anti-counterfeiting, Security, and Identification in Communication (ASID'09), Hong Kong, 20–22 Aug. 2009. — 2009. — PP. 160–162.
12. Peng, L. A blind image watermarking scheme based on wavelet tree quantization / L. Peng, D. Zhizhong // Second International Symposium on Electronic Commerce and Security (ISECS'09), 22–24 May 2009, Nanchang. — 2009. — Vol. 1. — PP. 218–222.
13. Коначович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Коначович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
14. Lu, W. Robust digital image watermarking based on subsampling / W. Lu, H. Lu, F.-L. Chung // Applied Mathematics and Computation. — 2006. — Vol. 181, Iss. 2. — PP. 886–893.
15. Nasir, I. Subsampling-based image watermarking in compressed DCT domain / I. Nasir *et al.* // The Tenth IASTED International Conference on Signal and Image Processing (SIP 2008), August 18 – 20, 2008, Kailua-Kona, Hawaii, USA. — 2008. — PP. 339–344.
16. Fan, C.-H. A robust watermarking technique resistant Jpeg compression / C.-H. Fan, H.-Y. Huang, W.-H. Hsu // Journal of Information Science and Engineering. — 2011. — Vol. 27, Iss. 1. — PP. 163–180.
17. Shahraeini, S. A Robust Digital Image Watermarking Approach against JPEG Compression Attack Based on Hybrid Fractal-Wavelet / S.Shahraeini, M.Yaghoobi // Proceedings of 8<sup>th</sup> International Conference on Computer Science and Information Technologies (CSIT 2011), 26–30 September, 2011, Yerevan, Armenia. — 2011. — Vol. 5. — PP. 616–622.
18. Колесников, М.В. Метод скрытой передачи данных в оптическом канале видеокамеры [Электронный ресурс] / М.В. Колесников // Инженерный вестник. — М. : ФГБОУ ВПО «МГТУ им. Н.Э. Баумана», 2013. — № 2. — Режим доступа: <http://engbul.bmstu.ru/doc/543251.html>.
19. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М. : Техносфера, 2006. — 1070 с.
20. Деммель, Д. Вычислительная линейная алгебра [Текст] : теория и приложения / Д. Деммель; Пер. с англ. Х.Д. Икрамова. — М. : Мир, 2001. — 430 с.

**ПІДВИЩЕННЯ ПРИХОВАНОЇ ПРОПУСКНОЇ СПРОМОЖНОСТІ СТІЙКИХ ДО СТИСКУ СТЕГАНОГРАФІЧНИХ АЛГОРИТМІВ ДЛЯ ДОВІЛЬНИХ ЗОБРАЖЕНЬ-КОНТЕЙНЕРІВ**

М.О. Мельник

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

Розроблений стеганографічний алгоритм, стійкий до атаки стиском, у тому числі, з малими коефіцієнтами якості. Як контейнер використовується цифрове зображення, збережене в довільному форматі. Розробка алгоритму проведена на основі існуючих аналогів, математичним базисом яких є загальний підхід до аналізу стану й технології функціонування інформаційних систем. Основною перевагою нового стеганоалгоритму є збільшення в 6 разів його прихованої пропускної спроможності, у порівнянні з алгоритмами, покладеними в його основу. Наведені результати обчислювального експерименту, що підтверджують високу ефективність декодування вбудованої інформації в умовах атаки стиском з малими коефіцієнтами якості на стеганоповідомлення.

**Ключові слова:** стеганографічний алгоритм, атака стиском, стеганоповідомлення, цифрове зображення, симетрична матриця, власні значення, власні вектори, спектральне розкладання

**INCREASE STEGANOGRAPHIC CAPACITY OF COMPRESSIVE STRENGTH ALGORITHMS FOR ARBITRARY COVER IMAGES**

Margaret A. Melnik

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

Developed steganographic algorithm is compressive strength algorithms for arbitrary cover images including attacks with low quality factor. Cover is digital image stored in arbitrary format. Development of proposed algorithm based on existing analogues that based on general approach to the analysis of the status and technology functioning of information systems. The main advantage of the new steganographic algorithm is 6 times increase of its capacity, compared with the algorithms which it is based. The results of computational experiment confirming the high performance decoding of embedded information by compression attacks with low quality factor.

**Keywords:** steganographic algorithm, compression attack, stegano message, digital image, symmetric matrix, eigenvalues, eigenvectors, spectral decomposition

# МОДЕЛЮВАННЯ ПРОЦЕСІВ ПРИПИНЕННЯ ГОРІННЯ МЕТОДОМ КЛІТИННИХ АВТОМАТІВ

М.О. Пустовіт

Академія пожежної безпеки імені Героїв Чорнобиля ДСНС України,  
вул. Онопрієнка, 8, Черкаси, 18034, Україна; e-mail: fire@fire.ck.ua

Розглянуто математичні моделі процесу припинення горіння. Вказано на основні відмінності моделей, наведені приклади їх застосування на практиці. Розроблено модель процесу припинення горіння на основі методу клітинних автоматів. Враховано припинення горіння при зниженні концентрації кисню, повного вигорання горючого навантаження та подачі водяних струменів на площу горіння.

**Ключові слова:** моделювання, припинення горіння, поширення пожежі, клітинні автомати, розпилені водяні струмені

## Актуальність проблеми

Вдосконалення підготовки персоналу оперативно-рятувальної служби цивільного захисту неможливе без впровадження в процес навчання комп'ютеризованих систем і тренажерів.

У такій галузі знань, де практично неможливо наочно відобразити складні процеси і явища, що відбуваються в реальному житті, комп'ютерне моделювання є особливо актуальним. Моделювання в процесі навчання можна розглядати не лише як спосіб узагальнення і представлення знань, але і як знаряддя (засіб) його формування.

Існуючі на сьогодні моделі гасіння пожеж, великий внесок у розвиток яких внесли Астахова І.Ф., Кошмаров Ю.А., Пузач С.В., Рижов А.М. та інші, та тренажерні системи на їх основі не реалізовувалися для цілей навчання. Вони спрямовані на рішення конкретних практичних задач пожежної безпеки, відображають окремі випадки горіння речовин і матеріалів в приміщеннях певної форми. При цьому вимагають для свого функціонування значного часу із-за великого об'єму проведених обчислень. А розроблені до теперішнього часу тренажерні системи розвитку пожеж у більшості випадків не містять у своїй основі досить адекватних моделей гасіння пожеж.

Аналіз існуючих математичних моделей гасіння пожеж дозволить обрати серед них найбільш ефективні та оптимальні для моделювання відповідних процесів та висунути вимоги для створення комп'ютеризованого тренажеру підготовки пожежного-рятувальника.

## Аналіз останніх досліджень і публікацій

Аналіз існуючих математичних моделей гасіння пожеж не виявив готових і апробованих рішень для використання в тренажерах, що значною мірою пов'язано з відсутністю достатньо відпрацьованих теорії і практики розв'язання подібних задач у рамках підготовки пожежного-рятувальника.

Авторами [1] описано загальний підхід до моделювання гасіння пожеж водяними струменями. У даній роботі було показано, як теорія займання пояснює використання

води для гасіння пожеж. Розроблено модель гасіння пожежі, у якій користувач встановлює критерій гасіння шляхом визначення кількості пального і температур стін.

У комп'ютерній програмі «INTMODEL», що реалізовує інтегральну математичну модель пожежі [2], загасання полум'я відбувається при значенні функції режиму пожежі [2, нерівність (2.21)]  $K = 0,01$ , тобто при концентрації кисню в приміщенні близько 3%. У роботі С.В. Пузача [3] – при концентрації кисню 8%. В обох роботах при виникненні вказаних умов загасання моделюється вмить на усій площі пожежі.

Така стрибкоподібна імітація, на нашу думку, при використанні в тренажері візуально сприйматиметься користувачем як процес нелогічний, невідповідний дійсності. Тому при моделюванні загасання полум'я варто використовувати імовірнісний підхід.

Дослідником [4] розроблена модель гасіння пожежі для використання у комп'ютерній програмі тренування керівника гасіння пожежі. У цій моделі не має значення, ведеться гасіння суцільними або розпиленними струменями, водою або піною. Кожен літр вогнегасної речовини, поданий за одну секунду, викликає зменшення площі пожежі за цю секунду на певну величину. У моделі фігурує величина  $W_H^M$  – об'єм вогнегасної речовини, необхідної для гасіння одного квадратного метра пожежі ( $л/м^2$ ), яка визначає вогнегасну здатність речовини. Різні фактори, що ускладнюють або спрощують гасіння, в конкретному випадку враховуються збільшенням або зменшенням цієї величини. Крім цього задаються гранична дальність гасіння (радіус роботи ствола) в метрах і витрата води зі ствола ( $q_{cm}$ ) у л/с.

У комп'ютерній програмі «КИС РТП», що розроблена С.В. Субачевим [5] реалізовано процес гасіння пожежі методом клітинних автоматів. В моделі враховано припинення горіння внаслідок вигорання пожежного навантаження, зниження концентрації кисню та подачі певної кількості води на гасіння пожежі. Основним недоліком є те, що в моделі не враховано зміна ефективності гасіння пожежі водою при різних кутах розпилення струменя, дальності струменя та ін.

## Постановка завдання

Метою дослідження є аналіз існуючих математичних моделей гасіння пожеж для використання в комп'ютеризованому тренажері підготовки пожежного-рятувальника.

Застосування таких систем дозволить відбити усю сукупність процесів і явищ в усій її складності і взаємозв'язках, значно знизити витрати на натурне моделювання пожеж, скоротити терміни і підвищити рівень підготовки фахівців до ухвалення ефективних рішень в області пожежної безпеки. Необхідність їх впровадження в процес професійної підготовки фахівців оперативно-рятувальної служби цивільного захисту неодноразово відбивалася в роботах Брушлинського М.М., Денисова А.М., Кафідова В.В., Коломійця Ю.І., Місюкевича М.С., Семикова В.Л., Соболева М.М. і інших.

При розробці математичної моделі припинення горіння варто окреслити основні вимоги:

1) Математична модель повинна враховувати вигорання пожежного навантаження, зниження концентрації кисню та подачі певної кількості води на гасіння пожежі.

2) Математична модель повинна враховувати зміну ефективності гасіння пожежі водою при різних кутах розпилення водяного струменя, дальності його подачі, нерівномірність розподілу капель в об'ємі струменя.

### Викладення основного матеріалу дослідження

Загасання полум'я в розробленій моделі пожежі відбувається по одній з наступних причин.

1) Внаслідок повного вигорання горючого навантаження на деякій розрахунковій одиниці площі (рис. 1).

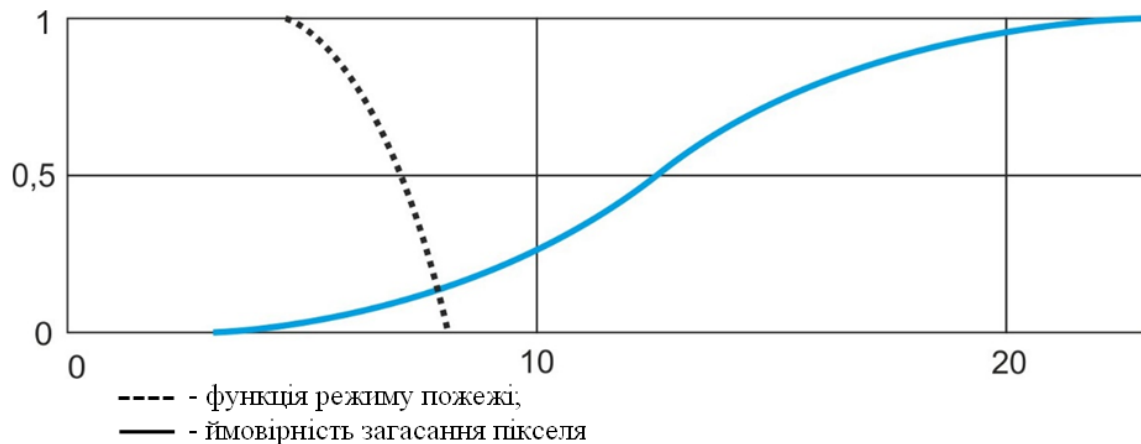
2) При зниженні концентрації кисню в приміщенні в результаті вільного горіння або в результаті подачі азоту або вуглекислого газу.

Ймовірність  $EXT\_PROB_1$ , загасання елемента на кожному кадрі анімації (кроці рахунку) внаслідок зниження концентрації кисню в приміщенні визначається формулою (1):

$$EXT\_PROB_1 = 1.1 - 6.25K, \quad (1)$$

де  $K$  — функція режиму пожежі.

Графічно залежність цієї ймовірності від концентрації кисню в приміщенні показана на рисунку 1.



**Рис. 1.** Залежність ймовірності загасання пікселя від концентрації кисню в приміщенні

3) Загасання полум'я імітується також при подачі на цю площу горіння певної витрати води. Причому час загасання залежить від відношення фактичної інтенсивності подачі води  $I_\phi$  до необхідної  $I_H$  (рис. 2):

$$\tau = \frac{10}{k^3} - 0.37, \quad (2)$$

де

$\tau$  — час, хв.;

$$k = \frac{I_\phi}{I_H}.$$

Необхідна інтенсивність подачі води на гасіння пожежі є відомою величиною та знаходиться за табл.11.1. [6]

Фактичну інтенсивність подачі води обчислюємо за наступною формулою:

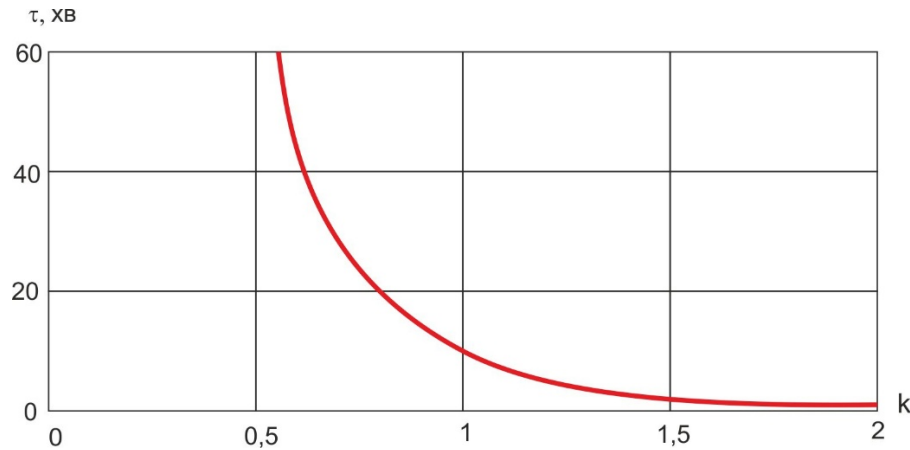


$$I_{\phi} = \frac{q_{ст}}{S_{пож}}, \quad (3)$$

де

$S_{пож}$  — площа пожежі, м<sup>2</sup>;

$q_{ст}$  — витрата води з пожежного ствола, л/с.



**Рис. 2.** Залежність часу загасання полум'я від відношення фактичної інтенсивності подачі води до необхідної

При такій залежності час загасання полум'я при подачі води необхідною інтенсивністю складає близько 10 хвилин.

Виходячи з кількості елементів в одному квадратному метрі площі,  $a = 1600 \text{ м}^2$ , і кількості кадрів рахунку в хвилину  $300 \text{ хв}^{-1}$  отримана формула, що описує залежність ймовірності загасання кожного елемента на поточному кроці рахунку від кратності  $k$ :

$$EXT\_PROB_2 = a \left[ \frac{-1}{300 \left( \frac{10}{k^3} - 0.37 \right)} \right] \quad (4)$$

На рисунку 3 показаний алгоритм обчислення ймовірності  $EXT\_PROB$  загасання кожного елемента залежно від концентрації кисню, інтенсивності подачі води і маси залишку горючого навантаження.

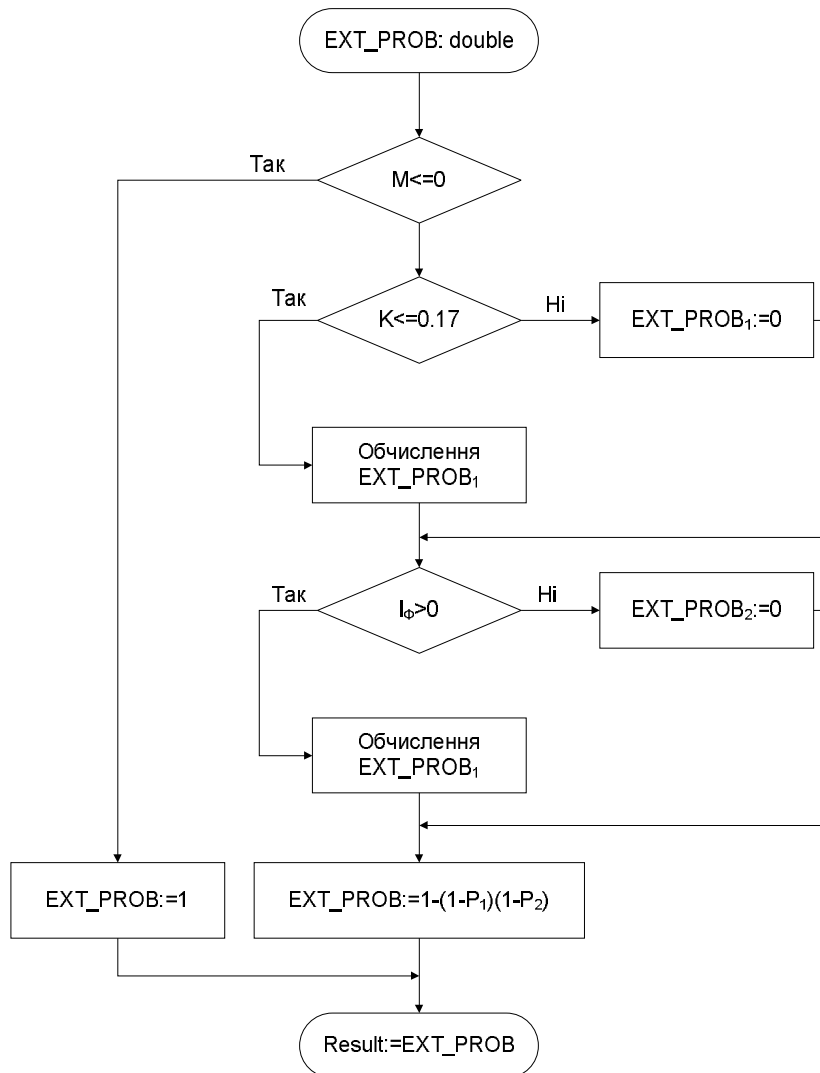
Окрім цього, у формулу (2) визначення ймовірності займання елемента доданий коефіцієнт, що зменшує лінійну швидкість поширення полум'я при подачі води, визначуваний по формулі:

$$k_v = \left( \frac{I_{\phi}}{I_H} - 1 \right) \quad (5)$$

Використання цього коефіцієнта дозволяє імітувати зниження лінійної швидкості поширення горіння при введенні перших засобів гасіння [6].

Так як було зазначено вище, для гасіння пожеж всередині будівель використовуються розпилені водяні струмені. Зважаючи на тактико-технічні

характеристики ми можемо визначити форму струменів та апроксимувати їх до умов нашої імовірнісної математичної моделі.



**Рис. 3.** Алгоритм обчислення ймовірності загасання кожного елементу FireList, що знаходиться в списку

Кут розпилювання стволів може змінюватись в межах 0,3-1,9 рад (30-110 град). Маючи ці дані, розраховуємо площу струменя (6)

$$S = \frac{\theta R^2}{2}, \quad (6)$$

де

- $\theta$  — кут розпилювання, рад;
- $R$  — довжина струменя.

Весь струмінь води не бере участь в припиненні горіння. Найбільш ефективно це робить розпилена фаза, що приблизно дорівнює 2/3 струменя. Тому площа струменя, що буде брати участь у гасінні обчислюється за наступною формулою (7)

$$S_{зас} = \frac{\theta R_1^2}{2} - \frac{\theta R_2^2}{2}, \quad (7)$$

де

$S_{зас}$  — площа водяного струменя, що бере участь в гасінні, м<sup>2</sup>;

$R_1$  — довжина струменя, м;

$R_2$  — довжина струменя, що не бере участь в гасінні пожежі.

Таким чином, отримуємо кількість елементів клітинного автомату, що на даний момент обробляються водою (8)

$$N_z = \frac{S_{зас}}{a}, \quad (8)$$

де  $a$  — кількість елементів у одному квадратному метрі.

Розподілення кількості води у площині струменя є нерівномірним. Найбільша кількість води знаходиться в центральній частині струменя, найменша – по краях струменя (рис. 4). Чим більша кількість води припадає на одну комірку клітинного автомату, тим більша фактична інтенсивність подачі води та швидкість переходу автомату зі стану «BURNING» в стан «EMPTY». Таким чином, формула (3) буде мати наступний вигляд:

$$l_\phi = \frac{q_{ef}}{S_{пож}}, \quad (9)$$

де  $q_{ef}$  — ефективна витрата води зі ствола в залежності від просторового положення КА відносно центру струменя

$$q_{ef} = q_{ст} \frac{|l_{КА}|}{R_{ст}}, \quad (10)$$

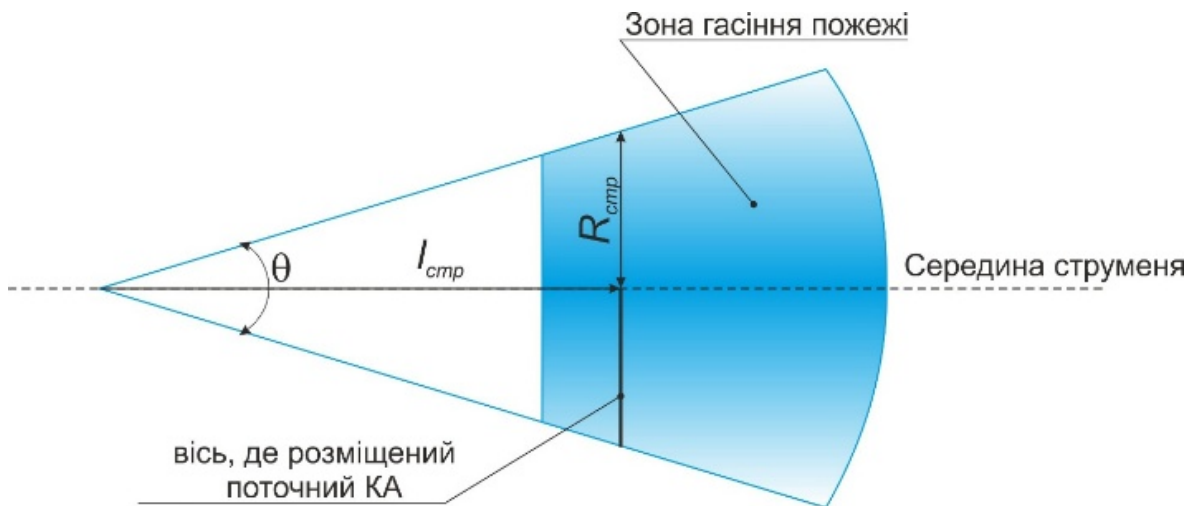
де

$l_{КА}$  — найкоротша відстань від КА до середини струменя, м;

$R_{ст}$  — радіус струменя, м

$$R_{ст} = l_{ст} \tan \frac{\theta}{2}, \quad (11)$$

де  $l_{ст}$  — довжина струменя води від краю ствола до осі з поточним КА, що перпендикулярна середині струменя.



**Рис.4.** Загальний вигляд розпиленого водяного струменя

## Висновки

Здійснений аналіз математичних моделей припинення горіння дав можливість оцінити їх основні переваги та недоліки для послідуєчого використання в комп'ютеризованому тренажері підготовки пожежного-рятувальника.

При розробці математичної моделі припинення горіння було враховано вигорання пожежного навантаження; зниження концентрації кисню та подачі певної кількості води на гасіння пожежі; зміну ефективності гасіння пожежі водою при різних кутах розпилення водяного струменя; дальності його подачі; нерівномірність розподілу капелів в об'ємі струменя

Подальшими перспективними дослідженнями є створення комплексної моделі розвитку та припинення горіння за допомогою методу клітинних автоматів для тривимірного простору, що дасть змогу візуалізувати вказані процеси та використати її в комп'ютеризованому тренажері підготовки пожежного-рятувальника

## Список літератури

1. Särđqvist, S. Water for Manual Fire Suppression / S. Särđqvist, G. Holmstedt // Journal of Fire Protection Engineering. — 2001. — Vol. 11, No. 4. — PP. 209–231.
2. Прогнозирование опасных факторов пожара [Текст] : лабораторный практикум / Ю.А. Кошмаров, Ю.С. Зотов, В.В. Андреев, С.В. Пузач. — М.: МИПБ МВД России, 1997. — 68 с.
3. Пузач, С.В. Методы расчета тепломассообмена при пожаре в помещении и их применение при решении практических задач пожаровзрывобезопасности : монография / С.В. Пузач ; Акад. гос. противопожар. службы и др. — М. : Акад. ГПС, 2005. — 336 с.
4. Разливанов, И.Н. Комплексная модель пожара и пожаротушения в условиях ограниченности сил и средств / И.Н. Разливанов // Проблемы прогнозирования чрезвычайных ситуаций. Сборник материалов VIII Всероссийской научно-практической конференции, Санкт-Петербург, 8–10 окт. 2008 г. — М.: Центр «Антистихия», 2008.
5. Субачев, С.В. Совершенствование подготовки персонала противопожарной службы на основе технологий имитационного моделирования пожаров в зданиях [Текст] : дис. ... канд. техн. наук : 05.13.10 / Субачев Сергей Владимирович. — М., 2008. — 113 с.
6. Теревнев, В.В. Справочник руководителя тушения пожара : такт. возможности пожар. подразделений / В.В. Теревнев ; М-во Рос. Федерации по делам гражд. обороны, чрезвычайн.

ситуациям и ликвидации последствий стихийн. бедствий, Акад. гос. противопожар. службы.  
— М. : ИБС-Холдинг, 2005. — 243 с.

### **МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ПРЕКРАЩЕНИЕ ГОРЕНИЯ МЕТОДОМ КЛЕТОЧНЫХ АВТОМАТОВ**

М.А. Пустовит

Академия пожарной безопасности имени Героев Чернобыля ГСЧС Украины,  
ул. Оноприенко, 8, Черкасы, 18034, Украина; e-mail: fire@fire.ck.ua

Рассмотрены математические модели процесса прекращения горения. Указаны основные отличия моделей, показаны примеры их использования на практике. Разработана модель процесса прекращения горения на основе метода клеточных автоматов. Учтено прекращение горения при снижении концентрации кислорода, полного выгорания горючего нагрузки и подачи водных струй на площадь горения.

**Ключевые слова:** моделирование, прекращение горения, распространение пожара, клеточные автоматы, распыленные водяные струи

### **MODELING THE PROCESSES OF BURNOUT BY CELLULAR AUTOMATA**

Mykhailo O. Pustovit

Academy of Fire Safety named after Chernobyl Heroes,  
8 Onoprienko str., Cherkassy, 18034, Ukraine; e-mail: fire@fire.ck.ua

The mathematical models of the extinguishing process were examined. Main differences between the models and examples of their use in practice were shown. The model of the burnout process on the basis of cellular automata is developed. Burnout while reducing the concentration of oxygen, complete combustion of the fuel load and the supply of water jets on the burning area is taken into account.

**Keywords:** modelling, burnout, fire spread, cellular automata, sprayed water jets

## АЛГОРИТМИ ОПРАЦЮВАННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ В КОМП'ЮТЕРНИХ СИСТЕМАХ

І.З. Якименко<sup>1</sup>, М.М. Касянчук<sup>1</sup>, Л.М. Тимошенко<sup>2</sup>, Н.Є. Гребень<sup>2</sup>

<sup>1</sup> Тернопільський національний економічний університет,  
вул. Львівська, 11, Тернопіль, 46029, Україна; e-mail: iyakymenko@mail.ru

<sup>2</sup> Одеський національний політехнічний університет,  
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: nata-sti4@mail.ru

Обґрунтовується використання теоретико-числового базису Крестенсона, що породжує систему числення залишкових класів, для реалізації алгоритмів опрацювання інформаційних потоків. Розроблені нові алгоритми модулярного множення в теоретико-числовому базисі Радемахера-Крестенсона, що дозволили зменшити складність з поліноміально-експоненційної до логарифмічної, що на один-два порядки збільшило швидкодію рішення задач даного класу. Наведені результати чисельних експериментів відповідають теоретично розрахованим параметрам і підтверджують правильність запропонованого наукового підходу.

**Ключові слова:** інформаційні потоки, теоретико-числовий базис Радемахера-Крестенсона, система залишкових класів, матрично-модулярне множення

### Вступ

Способи кодування інформаційних потоків визначаються теоретико-числовими базисами (ТЧБ), які застосовуються для їх представлення [1–3], найбільш поширеними з яких в сучасних комп'ютерних системах (КС) є наступні: унітарний, Хаара, Грея, Радемахера, Крестенсона та Галуа.

Світовий досвід створення процесорів для КС за останні 50 років, поряд з застосуванням ТЧБ Радемахера, який породжує двійкову систему числення, демонструє тенденцію все ширшого застосування інших ТЧБ, в тому числі: унітарного, Хаара, Крестенсона, Галуа, та сумісного використання комбінацій названих ТЧБ, наприклад Радемахера-Хаара, Крестенсона-Галуа тощо [4].

У зв'язку з цим існує проблема глибокого дослідження характеристик «нерадемахівських» ТЧБ та граничних можливостей їх застосування. При цьому перспективним, крім найбільш сьогодні масового одновимірного (векторного) представлення чисел та виконання операцій у ТЧБ Радемахера, є застосування двовимірних систем числення, вертикальної інформаційної технології у базисі Галуа та різних форм багатовимірного представлення чисел у вигляді залишків різних форм системи залишкових класів ТЧБ Крестенсона [5, 6].

Система числення залишкових класів (СЗК) ТЧБ Крестенсона, розроблена Акушським І.Я. та Юдіцьким Д.І., особливо її цілочисельна форма, широко використовувалась, починаючи з 70-х років минулого століття для побудови швидкодіючих спеціалізованих процесорів систем повітряної оборони колишнього СРСР [7]. Нормалізована форма СЗК, запропонована науковою школою професора Николайчука Я.М., активно використовується та застосовується при дослідженні двовимірних (матричних) форм систем числення ТЧБ Радемахера та Галуа [8].

## Мета та задачі дослідження

Досягнення необхідного рівня захисту інформації в КС, які розвиваються, обґрунтовує перспективу удосконалення алгоритмів формування та опрацювання інформаційних потоків. Для досягнення мети удосконалення та підвищення ефективності захисту інформаційних потоків необхідно вирішити ряд задач:

- дослідити теоретичні засади опрацювання інформаційних потоків;
- розробити швидкодіючі алгоритми опрацювання інформаційних потоків на основі різних ТЧБ;
- створити спеціалізовані програмні засоби опрацювання інформаційних потоків.

## Теоретичні засади використання системи залишкових класів

Відомо, що двійкова система числення, яка використовується в сучасних комп'ютерних системах, має певні недоліки – наявність міжрозрядних зв'язків та велику розрядність [9]. Тому актуальним є розвиток і застосування непозиційних систем числення, в яких відсутні вказані недоліки. Прикладом може бути СЗК, або, як її ще називають, представлення чисел у базисі Крестенсона [10], [11], причому найбільш фундаментально досліджено цілочисельну форму в системі залишкових класів. Хоча вона не набула значного поширення у зв'язку з необхідністю визначення умов переповнення, складністю та громіздкістю зворотнього перетворення чисел у десяткову систему числення, а також складнощами реалізації операцій ділення та порівняння, але СЗК можна ефективно використовувати у мультибазисних процесорах, спеціалізованих обчислювальних машинах для виконання операцій додавання, віднімання та множення, наприклад, у задачах лінійної алгебри (матрично-векторні операції) тощо. Необхідно відмітити, що ця система особливо ефективна при обчисленнях з великими числами [12], [13].

Фундаментальною основою СЗК є теорія чисел [14], зокрема, властивості китайської теореми про залишки. Будь-яке ціле додатне число  $N$  у десятковій системі числення представляється в СЗК у вигляді набору найменших додатніх залишків від ділення цього числа на фіксовані цілі додатні попарно взаємно прості числа  $p_1, p_2, \dots, p_n$  ( $N_{10} = (b_1, b_2, \dots, b_n)_{p_1, p_2, \dots, p_n}$ , де  $b_i = N \bmod p_i$ ), які називаються модулями ( $n$  — кількість модулів). При цьому повинна виконуватись умова  $0 \leq N \leq P-1$ , де

$$P = \prod_{i=1}^n p_i.$$

На відміну від позиційних систем числення, де величина визначеного розряду суми, різниці або множення залежить не тільки від значень відповідних, але і від попередніх розрядів доданків або множників, в СЗК додавання, віднімання та множення цілих чисел виконується окремо по кожному модулю і переноси між розрядами відсутні. Отже, такі операції в СЗК є модульними [15].

Нехай два десяткові числа  $A$  і  $B$ , записані в СЗК за вибраними модулями:

$$A_{10} = (a_1, a_2, \dots, a_i, \dots, a_n)_{p_1, p_2, \dots, p_i, \dots, p_n},$$

$$B_{10} = (b_1, b_2, \dots, b_i, \dots, b_n)_{p_1, p_2, \dots, p_i, \dots, p_n}.$$

Тоді:

$$A_{10} \pm B_{10} = C_{10} = (c_1, c_2, \dots, c_i, \dots, c_n)_{p_1, p_2, \dots, p_i, \dots, p_n},$$

$$A_{10} \times B_{10} = D_{10} = (d_1, d_2, \dots, d_i, \dots, d_n)_{p_1, p_2, \dots, p_i, \dots, p_n}$$

де

$$c_i = a_i \pm b_i,$$

$$d_i = a_i \times b_i.$$

Останні рівності справедливі лише в тому випадку, коли результат операції не виходить за межі інтервалу  $\prod_{i=1}^n p_i - 1$ .

Зворотне перетворення із ТЧБ Крестенсона у десяткову систему числення є досить громіздким і ґрунтується на використанні китайської теореми про залишки [14]:

$$N = \left( \sum_{i=1}^n b_i B_i \right) \bmod P, \quad (1)$$

де  $B_i = M_i m_i$ ,  $M_i = \frac{P}{p_i}$ ,  $m_i$  шукається з виразу  $(M_i m_i) \bmod p_i = 1$ , при цьому повинна

виконуватись умова  $\left( \sum_{i=1}^n B_i \right) \bmod P = 1$ .

Слід зазначити, що при переведенні чисел із СЗК у десяткову систему числення значну обчислювальну складність становить пошук коефіцієнтів  $m_i = M_i^{-1} \bmod p_i$ . У роботі [8] розглянуто досконалу форму СЗК (ДФ СЗК), у якій підбір модулів такий, що  $m_i = 1$ , тобто

$$M_i \bmod p_i = 1. \quad (2)$$

Подальший розвиток ДФ СЗК отримала у роботах [16, 17], у яких було встановлено правила побудови наборів з будь-якої кількості модулів ДФ СЗК для будь-якого діапазону десяткових чисел. Шукані модулі повинні отримуватися з такої умови:

$$\begin{cases} p_1 = 2 \\ p_i = p_1 p_2 \dots p_{i-1} + 1, 1 < i < n. \\ p_n = p_1 p_2 \dots p_{n-1} - 1. \end{cases} \quad (3)$$

Слід зазначити, що запропонована система не вичерпує всіх можливих наборів для ТЧБ Крестенсона при заданих  $n$ . Набір модулів, отриманий за допомогою системи (3), найоптимальніший, оскільки в цьому випадку величина  $P$  є максимальна, що дозволяє розглядати найбільший діапазон десяткових чисел. При цьому досягається зменшення розрядності вдвічі.

Крім того, у цих роботах запропонована напівдосконала форма СЗК ( $m_i = \pm 1$ ), яку зручно використовувати у випадку обмеженої кількості модулів та необхідності розгляду великих чисел. Перспективними модифікаціями СЗК, які на даний час досліджуються, є нормалізована та розмежована форми СЗК.

Отже, переваги представлення чисел у базисі Крестенсона для опрацювання інформаційних потоків в КС очевидні – виконання операцій над великорозрядними числами, які представляються залишками, а не над великими числами базису Радемахера.



## Алгоритм модулярного множення у ТЧБ Радемахера–Крестенсона

У роботі [18] викладені теоретичні основи виконання операцій модулярного множення та експоненціювання при застосуванні теоретико-числових базисів Радемахера та Крестенсона та отримано аналітичні вирази обчислювальної складності запропонованих високопродуктивних алгоритмів.

Запропоновано алгоритм матрично-модулярного множення  $n$ -розрядних чисел  $a = a_{n-1}2^{n-1} + \dots + a_i2^i + \dots + a_12 + a_0$  та  $b = b_{n-1}2^{n-1} + \dots + b_j2^j + \dots + b_12 + b_0$ , де  $a_i, b_j = 0, 1$ ,  $n$  — розрядність модуля  $p$ . Після побудови матриці  $\|c_{ij}\| = 2^{i+j} \bmod p$  добуток чисел  $a$  та  $b$  отримується згідно формули:

$$a \cdot b = \left( \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} a_i b_j 2^{i+j} \right) \bmod p, \quad (4)$$

де  $a_i, b_j = 1$ , тобто  $c_{ij}$  знаходиться на перетині стовпця та рядка, для яких відповідні  $a_i$  та  $b_j$  дорівнюють 1.

Модулярне множення в ТЧБ Радемахера–Крестенсона здійснюється згідно наступного алгоритму.

**Вхід:**  $a = a_{n-1}2^{n-1} + \dots + a_i2^i + \dots + a_12 + a_0$ ,  $b = b_{n-1}2^{n-1} + \dots + b_j2^j + \dots + b_12 + b_0$ ,  $a_i, b_j = 0, 1$ ,  $n$  — розрядність модуля  $p$ .

1) Знаходимо залишки кожного біта  $a$  і  $b$  по заданому модулю  $p$ .

2) Сумуємо залишки останньої стрічки матриці розкладу чисел  $a$  і  $b$  по модулю  $p$ .

Отримуємо  $c_n$ .

3) Помножуючи  $c_n \cdot 2$  за модулем  $p$  і пропускаючи нульові стрічки, записуємо вектор стовпчик  $c_i$ . Отримуємо вектор залишків  $a \cdot b \pmod{p}$ .

**Вихід:**  $c_i$ .

Блок-схема алгоритму представлена на рис. 1. Отриманий алгоритм заміни операції множення, яка має квадратичну обчислювальну складність  $O1(n) = n^2$ , матрично-модульною операцією сумування в ТЧБ Радемахера–Крестенсона з логарифмічною складністю

$$O2(n) = \begin{cases} (\log_2 n)^2, & \text{якщо } n < 256 \\ n \cdot (\log_2 n), & \text{в інших випадках} \end{cases}$$

Основна перевага розробленого алгоритму по відношенню до існуючих – заміна багатотактної операції множення на однокітну сумування залишків. Алгоритм дозволяє реалізувати матриці розрядності 1024 біти за 2-4 мс, що при тактовій частоті процесора  $10^9$  прискорює реалізацію алгоритму в 20-40 разів.

## Удосконалений алгоритм модулярного множення на основі використання ТЧБ Радемахера–Крестенсона

Для виконання операції модулярного множення  $a \cdot b \pmod{p}$  двох  $n$ -розрядних чисел, представимо числа  $a$  та  $b$  в двійковій системі числення базису Радемахера, тобто:

$$a = \sum_{i=1}^{n-1} a_i 2^i = a_0 2^0 + a_1 2^1 + a_2 2^2 + \dots + a_{n-1} 2^{n-1},$$

$$b = \sum_{j=1}^{n-1} b_j 2^j = b_0 2^0 + b_1 2^1 + b_2 2^2 + \dots + b_{n-1} 2^{n-1},$$

де

$$a_i = 0.1;$$

$$b_j = 0.1;$$

$n$  — розрядність модуля  $p$ .

Для знаходження результату їх множення за модулем  $p$  побудуємо матрицю, представлену в табл. 1, де  $k_j = 2^j \bmod p$ .

**Таблиця 1.**

Матриця множення в ТЧБ Радемахера–Крестенсона

|           |           |       |           |       |           |           |       |       |       |
|-----------|-----------|-------|-----------|-------|-----------|-----------|-------|-------|-------|
|           | $k_{n-1}$ |       | $k_1$     | $k_0$ | .....     | $k_{n-1}$ |       | $k_1$ | $k_0$ |
| $a_{n-1}$ | $b_{n-1}$ |       | $b_1$     | $b_0$ | 0         | 0         | 0     | 0     | 0     |
| ...       | 0         | ..... | .....     | ..... | .....     | 0         | 0     | 0     | 0     |
| $a_i$     | 0         | 0     | $b_{n-1}$ |       | $b_1$     | $b_0$     | 0     | 0     | 0     |
| ...       | 0         | 0     | 0         | ..... | .....     | .....     | ..... | 0     | 0     |
| $a_1$     | 0         | 0     | 0         | 0     | $b_{n-1}$ |           | $b_1$ | $b_0$ | 0     |
| $a_0$     | 0         | 0     | 0         | 0     | 0         | $b_{n-1}$ |       | $b_1$ | $b_0$ |

$$a \cdot b(\bmod p) = a_0 b_0 k_0 + (a_0 b_1 + a_1 b_0) k_1 + (a_0 b_2 + a_1 b_1 + a_2 b_0) k_2 + \dots + (a_0 b_{n-1} + a_1 b_{n-2} + \dots + a_{n-1} b_0) k_i \tag{6}$$

Позначимо через:

$$A_l = (a_0 b_{n-1} + a_1 b_{n-2} + \dots + a_{n-1} b_0) k_l, \tag{7}$$

$$a \cdot b(\bmod p) = \sum_{l=1}^{2n} A_l \bmod p. \tag{8}$$

З врахуванням (7) співвідношення (8) набуде вигляду:

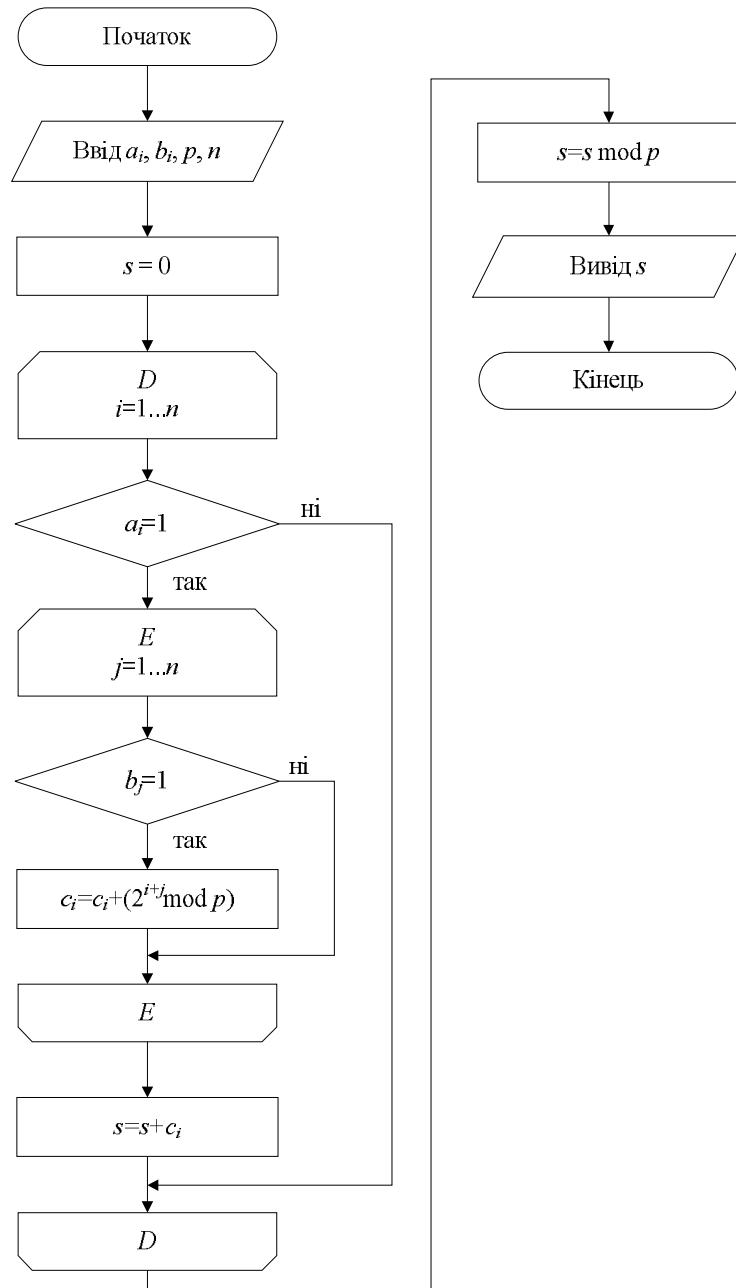
$$a \cdot b(\bmod p) = \left( \sum_{l=1}^{2n} \left( \sum_{\substack{i=0 \\ j=0}}^{n-1} a_i b_j \right) k_l \right) \bmod p, \tag{9}$$

$$i + j = n - 1.$$

Причому, якщо  $a_i = 1, b_s, b_q = 1$ , тоді отримуємо спрощення при розрахунку операції модулярного множення з використанням наступного співвідношення:

$$(b_s + b_q)k_i = k_{i+1} \quad (10)$$

Отже, при використанні співвідношення (10) суттєво зменшується обчислювальна складність виконання операції модулярного множення, що дозволяє ефективно використовувати запропонований метод в алгоритмах захисту інформаційних потоків, побудованих на асиметричних криптосистемах.



**Рис. 1.** Блок схема алгоритму модулярного множення в ТЧБ Радемахера-Крестенсона

Розглянемо приклад: знайти значення виразу  $21 \cdot 25 \bmod 29$ .

Для початку представляємо числа 21 і 25 в двійковій системі числення, тобто  $21=10101$ ,  $25=11001$ , тоді на основі використання табл. 1 отримуємо:

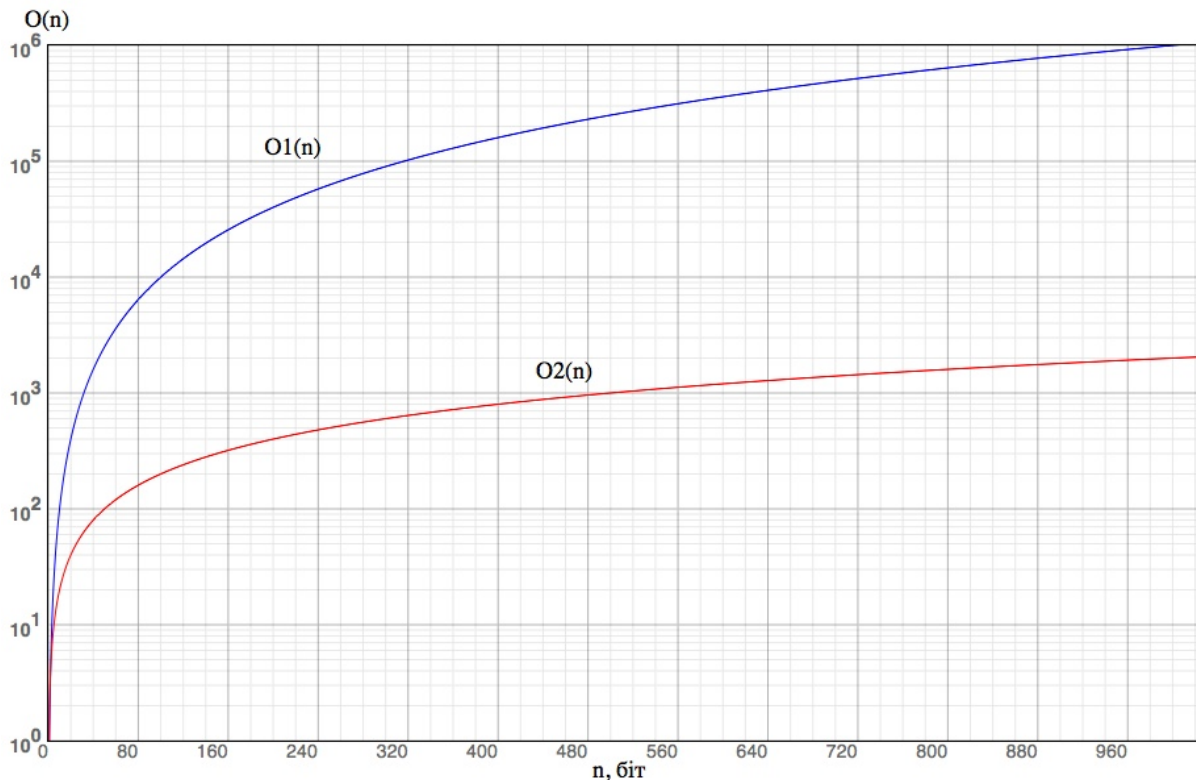
|   |    |    |    |   |   |    |   |   |   |   |
|---|----|----|----|---|---|----|---|---|---|---|
|   | 19 | 24 | 12 | 6 | 3 | 16 | 8 | 4 | 2 | 1 |
| 1 |    | 1  | 0  | 1 | 0 | 1  |   |   |   |   |
| 1 |    |    | 1  | 0 | 1 | 0  | 1 |   |   |   |
| 0 |    |    |    |   |   |    |   |   |   |   |
| 0 |    |    |    |   |   |    |   |   |   |   |
| 1 |    |    |    |   |   | 1  | 0 | 1 | 0 | 1 |

З врахуванням співвідношення (10) одержимо

$$(24+12+6+16+16+8+4+1)\text{mod}29=(19+8+4+1)\text{mod}29=3.$$

Таким чином, отримано удосконалений новий алгоритм заміни операції множення, яка має квадратичну обчислювальну складність  $O1(n) = n^2$ , матрично-модульною операцією сумування в ТЧБ Радемахера–Крестенсона з лінійною складністю  $O2(n) = 2n$ .

Результати дослідження обчислювальної складності запропонованого алгоритму наведені на рисунку 2.



**Рис. 2.** Обчислювальна складність операції модулярного множення удосконаленого алгоритму на основі використання ТЧБ Радемахера–Крестенсона

Результати чисельного експерименту показують, що розроблений метод характеризується на 1 порядок меншою обчислювальною складністю по відношенню до відомих і дозволяє ефективно застосовувати його в різного роду задачах, наприклад в асиметричних системах захисту на етапах як генерування ключів, так і шифрування/дешифрування даних.

## Висновки

Розроблені нові алгоритми опрацювання інформаційних потоків – модулярного множення в ТЧБ Радемахера-Крестенсона дозволили зменшити складність з поліноміально-експоненційної до логарифмічної та лінійної, що на 1-2 порядки збільшило швидкодію рішення задач даного класу. Розроблені інструментальні програмні засоби реалізації алгоритмів модулярного множення дали можливість дослідити вплив часової складності на характеристики запропонованих алгоритмів. Результати відповідають теоретично розрахованим параметрам і підтверджують правильність та результативність запропонованого наукового підходу по вдосконаленню алгоритмів опрацювання інформаційних потоків в комп'ютерних системах.

Оскільки операція модулярного множення є базовою в найбільш поширених системах захисту інформаційних потоків з відкритими ключами, то доцільно використовувати розроблений метод в задачах захисту інформаційних потоків на практиці для вдосконалення систем захисту інформаційних потоків.

## Список літератури

1. Блейхут, Р. Быстрые алгоритмы цифровой обработки сигналов [Текст] = Fast algorithms for digital signal processing : таблицы / Р.Э. Блейхут ; пер. И.И. Грушко ; ред.: В.И. Арнольд, А.С. Попов ; худож. А. Рейнце, пер. с англ. — Москва : Мир, 1989. — 448 с.
2. Николайчук, Я.М. Теорія джерел інформації [Текст] : монографія / Я.М. Николайчук. — Т. : ТНЕУ, 2008. — 536 с.
3. Литвин, А.И. Организация векторных вычислений спектральных коэффициентов преобразования Хаара / А.И. Литвин, А.И. Май, Л.А. Писаренко // Тезисы докладов международной конференции по вычислительной математике (МКВМ-2002), 24–28 июня 2002 г., Новосибирск, Академгородок. — Новосибирск, 2002. — С. 46–58.
4. Николайчук, Я.М. Теоретичні основи побудови та структура спецпроцесорів в базисі Крестенсона / Я.М. Николайчук, О.І. Волинський, С.В. Кулина // Вісник Хмельницького національного університету. — Хмельницький, 2007. — № 3, Т. 1. — С. 85–90.
5. Алексеев, В.Е. Графы и алгоритмы. Структуры данных. Модели вычислений [Текст] : учеб. для студ., обуч. по спец. 010200 – «Прикладная математика и информатика» и по напр. 510200 – «Прикладная математика и информатика» / В.Е. Алексеев, В.А. Таланов. — М. : ИНТУИТ : БИНОМ. ЛЗ, 2006. — 320 с.
6. Столлингс, В. Структурная организация и архитектура компьютерных систем: Проектирование и производительность [Текст] = Computer organization and architecture: Designing and Performance : монографія / В. Столлингс; [Пер. с англ. и ред. В.Т. Тертышного]. — 5-е изд. — М. : Вильямс, 2002. — 892 с.
7. Николайчук Я.М. Основи побудови часових систем на базі вертикальної інформаційної технології / Я.М. Николайчук // Тези науково-практичної конференції професорсько-викладацького складу. — Івано-Франківськ, 1999. — С. 90–92.
8. Николайчук, Я.М. Матричні системи числення / Я.М. Николайчук, О.Д. Круцкевич // Вісник Хмельницького національного університету. — Хмельницький, 2007. — № 3, Т. 1. — С. 62–64.
9. Акушский, И.Я. Машинная арифметика в остаточных классах [Текст] : монографія / И.Я. Акушский, Д.И. Юдицкий. — М. : Советское радио, 1968. — 439 с.
10. Касянчук, М.М. Теорія та оптимізація алгоритмів опрацювання великорозрядних чисел у базисі Крестенсона / М.М. Касянчук, І.З. Якименко, С.В. Івасьєв // Вісник Хмельницького національного університету. — Хмельницький, 2011. — № 3. — С. 265–273.
11. Корнилов, А.И. Принципы построения модулярных индексных умножителей // А.И. Корнилов, М.Ю. Семенов, О.В. Ласточкин // Известия высших учебных заведений. Электроника. — 2004. — № 2. — С. 48–55.
12. Задірака, В.К. Комп'ютерна арифметика багаторозрядних чисел: наукове видання / В.К. Задірака, О.С. Олексюк. — Київ, 2003. — 264 с.
13. Локазюк, В.М. Контроль і діагностування часових пристроїв та систем : Навчальний посібник для ВУЗів. — Хмельницький : ТУП, 2001. — 242 с.

14. Бородин, О.І. Теорія чисел : підручник / О.І. Бородин. — вид. 3-ге, перероб. і допов. — Київ : Вища школа, 1970. — 275 с.
15. Торгашев, В.А. Система остаточных классов и надежность ЦВМ [Текст] : научное издание / В.А. Торгашев. — Москва : Сов. радио, 1973. — 120 с.
16. Касянчук, М.М. Теорія та математичні закономірності досконалої форми системи залишкових класів / М.М. Касянчук / Праці Міжнародного симпозиуму «Питання оптимізації обчислень (ПОО–XXXV)». — Київ–Кацивелі, 2009. — Т. 1. — С. 306–310.
17. Kasyanchuk, M. Conception of theoretical bases of the accomplished form of Krestenson's transformation and its practical application / M. Kasyanchuk / Proceedings of the 4<sup>th</sup> International Conference «Advanced Computer Systems and Networks: Design and Application» (ACSN–2009). — Lviv (Ukraine), 2009. — PP. 299–301.
18. Николайчук Я.М. Теоретичні основи виконання модулярних операцій множення та експоненціювання в теоретико-числовому базисі Крестенсона-Радемахера / Я.М. Николайчук, М.М. Касянчук, І.З. Якименко, Т.М. Долинюк // Інформатика та математичні методи в моделюванні. — 2011. — Том 1, № 2. — С. 123–130.

## АЛГОРИТМЫ ОБРАБОТКИ ИНФОРМАЦИОННЫХ ПОТОКОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

И.З. Якименко<sup>1</sup>, М.Н. Касянчук<sup>1</sup>, Л.Н. Тимошенко<sup>2</sup>, Н.Е. Гребень<sup>2</sup>

<sup>1</sup> Тернопольский национальный экономический университет,  
ул. Львовская, 11, Тернополь, 46020, Украина; e-mail: iyakymenko@mail.ru

<sup>2</sup> Одесский национальный политехнический университет,  
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: nata-sti4@mail.ru

Обосновывается использование теоретико-числового базиса Крестенсона, порождающего систему исчисления остаточных классов, для реализации алгоритмов обработки информационных потоков. Разработаны новые алгоритмы модулярного умножения в теоретико-числовом базисе Радемахера-Крестенсона, что позволило уменьшить сложность с полиномиальной-экспоненциальной до логарифмической, что на один-два порядка увеличило быстродействие решения задач данного класса. Приведенные результаты численных экспериментов соответствуют теоретически рассчитанным параметрам и подтверждают правильность предложенного научного подхода.

**Ключевые слова:** информационные потоки, теоретико-числовой базис Радемахера-Крестенсона, система остаточных классов, матрично-модулярное умножение

## ALGORITHMS OF PROCESSING OF INFORMATION FLOWS IN COMPUTER SYSTEMS

Igor Z. Yakimenko<sup>1</sup>, Michael N. Kasyanchuk<sup>1</sup>, Lidiya M. Timoshenko<sup>2</sup>, Nataliya E. Greben<sup>2</sup>

<sup>1</sup> Ternopil National Economic University,  
11 Lvivska str., Ternopil, 46020, Ukraine; e-mail: iyakymenko@mail.ru

<sup>2</sup> Odessa National Polytechnic University,  
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: nata-sti4@mail.ru

The using of Rademacher-Krestenson's basis is justified for realization of algorithms of information flows processing. New algorithms of modular multiplication in the theoretical and numerical Rademacher-Krestenson's basis are developed. It helped reduce the complexity from polynomial or exponential to logarithmic. The theoretically calculated parameters are confirmed by the results of numerical experiments.

**Keywords:** information flows, Rademacher-Krestenson's basis, residual classes system, matrix and modular multiplication

# АНАЛИЗ ПРЕИМУЩЕСТВ ПРОСТРАНСТВЕННОЙ ОБЛАСТИ ЦИФРОВОГО ИЗОБРАЖЕНИЯ-КОНТЕЙНЕРА ДЛЯ СТЕГАНОПРЕОБРАЗОВАНИЯ

О.В. Костырка

Академия пожарной безопасности имени Героев Чернобыля ГСЧС Украины,  
ул. Оноприенко, 8, Черкассы, 18034, Украина; e-mail: chaykaov@rambler.ru

В работе проведен детальный анализ преимуществ использования для стеганопреобразования пространственной области изображения-контейнера по сравнению с областью преобразования. В ходе анализа получены оценки вычислительной сложности перевода изображения из пространственной области в области различных преобразований, наиболее часто используемых в стеганографии, а также оценки вычислительной погрешности, возникающей в результате выполнения прямого и обратного преобразования изображения. Установлено, что пространственная область изображения-контейнера является предпочтительной по сравнению с областью преобразования для внедрения дополнительной информации с точки зрения оценки вычислительной сложности и вычислительной погрешности.

**Ключевые слова:** цифровое изображение, пространственная область, область преобразования изображения, вычислительная сложность, вычислительная погрешность, стеганопреобразование

## Введение

Цифровые изображения (ЦИ) сегодня часто используются в качестве контейнеров в стеганографии. Одной из причин этого является возможность изменений матрицы/матриц изображения, происходящих в процессе стеганопреобразования (СП), без нарушений его надежности восприятия.

Для погружения дополнительной информации (ДИ) в контейнер-изображение могут использоваться как пространственная, так и область преобразования ЦИ. В качестве области преобразования может, в частности, выступать частотная область ЦИ [1, 2], область различных разложений матрицы: сингулярного, спектрального [3, 4], и др. [5, 6].

На протяжении долгого времени считалось, что для обеспечения помехоустойчивости стеганографических методов и алгоритмов предпочтительной для погружения ДИ является область преобразования изображения, в частности, частотная область. Это утверждение в свете работ [7,8] является ошибочным, поскольку в них показано, что не имеет значения, в какой области контейнера происходит погружение ДИ; важно, к каким возмущениям сингулярных чисел (СНЧ) и сингулярных векторов (СНВ) матрицы контейнера это приведет, где эти возмущения будут локализованы. Очевидно, что кажущееся преимущество стеганоалгоритмов, погружающих ДИ в области преобразования, основано на том, что реализовать полученные в [8] достаточные условия устойчивости стеганоалгоритма к возмущающим воздействиям в пространственной области сложнее, чем в области преобразования, но принципиально возможно.

Пространственная область изображения-контейнера при разработке стеганоалгоритмов на сегодняшний день несправедливо отходит на второй план. Исключение

составляет, пожалуй, лишь метод модификации наименьшего значащего бита, осуществляющий погружение ДИ в пространственной области, широко используемый до настоящего момента, но и он претерпевает в последнее время модификации, связанные с организацией СП в области дискретного косинусного преобразования (ДКП).

По мнению автора, учитывая принципиальную возможность построения устойчивых к возмущающим воздействиям стеганометодов независимо от используемой для СП области контейнера, основное внимание при разработке алгоритмов сегодня необходимо уделять именно пространственной области для организации внедрения ДИ, очередным аргументом чего и является настоящая работа.

### Цель статьи и постановка заданий

Целью статьи является детальный анализ преимуществ использования для стеганопреобразования пространственной области контейнера-изображения, по сравнению с областью преобразования.

Для достижения цели необходимо решить следующие задачи:

1) Оценить «накладные» вычислительные расходы для перевода ЦИ из пространственной области в области преобразования, наиболее часто используемые в стеганографии;

2) Оценить вычислительную погрешность, возникающую при выполнении прямого и обратного преобразования изображения вида: «пространственная область – область преобразования (ПО – ОП)», «область преобразования – пространственная область (ОП – ПО)».

### Основная часть

Наиболее часто используемыми на сегодняшний день преобразованиями ЦИ, предваряющими погружение ДИ, являются:

- дискретное косинусное преобразование (ДКП);
- вейвлет-преобразование (ВП);
- сингулярное/спектральное разложение матрицы ЦИ.

Любая предобработка ЦИ потребует дополнительных вычислительных затрат. Оценим эти затраты для перечисленных выше преобразований.

Пусть матрица контейнера  $F$  с элементами  $f_{ij}$  имеет размеры  $m \times m$  пикселей ( $i, j = \overline{0, m-1}$ ). С учетом того, что прямое ДКП с матрицей  $T$ , элементы которой ниже обозначаются как  $t_{uv}$ , выражается в виде [9]:

$$t_{uv} = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} f_{ij} \alpha(u) \alpha(v) \cos\left(\frac{(2i+1)u\pi}{2m}\right) \cos\left(\frac{(2j+1)v\pi}{2m}\right),$$

для  $u, v = \overline{0, m-1}$ , где

$$\alpha(u) = \begin{cases} \sqrt{1/m} & \text{для } u = 0 \\ \sqrt{2/m} & \text{для } u = 1, 2, \dots, m-1 \end{cases},$$

и аналогично для  $\alpha(v)$ , а обратное может быть представлено как



$$f_{ij} = \sum_{u=0}^{m-1} \sum_{v=0}^{m-1} t_{uv} \alpha(u) \alpha(v) \cos\left(\frac{(2i+1)u\pi}{2m}\right) \cos\left(\frac{(2j+1)v\pi}{2m}\right),$$

то процесс ПО – ОП, ОП – ПО в случае ДКП в «классическом виде» потребует

$$S = \underline{O}(m^4) \quad (1)$$

операций, что на порядок превосходит вычислительную сложность процесса получения сингулярного/спектрального разложения матрицы  $F$ .

Для большинства современных стеганоалгоритмов перед погружением ДИ матрица контейнера разбивается на блоки различного фиксированного размера  $n \times n$  (чаще всего –  $8 \times 8$  пикселей), после чего каждый блок подвергается СП. Предобработкой блока может служить перевод его из пространственной области в область преобразования, на что затрачивается определенное, не зависящее от размера матрицы контейнера, количество операций  $K$ . Тогда общее число операций, которое потребуется для перевода всех блоков в область преобразования, определяется количеством блоков и составляет:

$$S = K \left[ \frac{m}{n} \right] \left[ \frac{m}{n} \right] = \underline{O}(m^2), \quad (2)$$

операций, где  $[ \bullet ]$  — целая часть аргумента. Такое же количество операций потребуется и для обязательного обратного перехода из области преобразования в пространственную область изображения.

При учете того, что реальные ЦИ имеют значительные размеры, значительными оказываются и «накладные вычислительные расходы» (1), (2) для процессов ПО – ОП, ОП – ПО.

Формулы (1), (2) дают решение задачи 1 в списке решаемых задач.

Особенности машинной арифметики накладывают свои отпечатки на вычисления, производимые в системе с плавающей точкой. Нельзя не учитывать тот факт, что вычисления, связанные с переходом в область преобразования ЦИ, вносят дополнительную погрешность в любой процесс, связанный с возвращением в пространственную область, что обязательно происходит при стеганопреобразовании.

Рассмотрим в этой связи детально каждое из вышеперечисленных преобразований, начиная с ДКП.

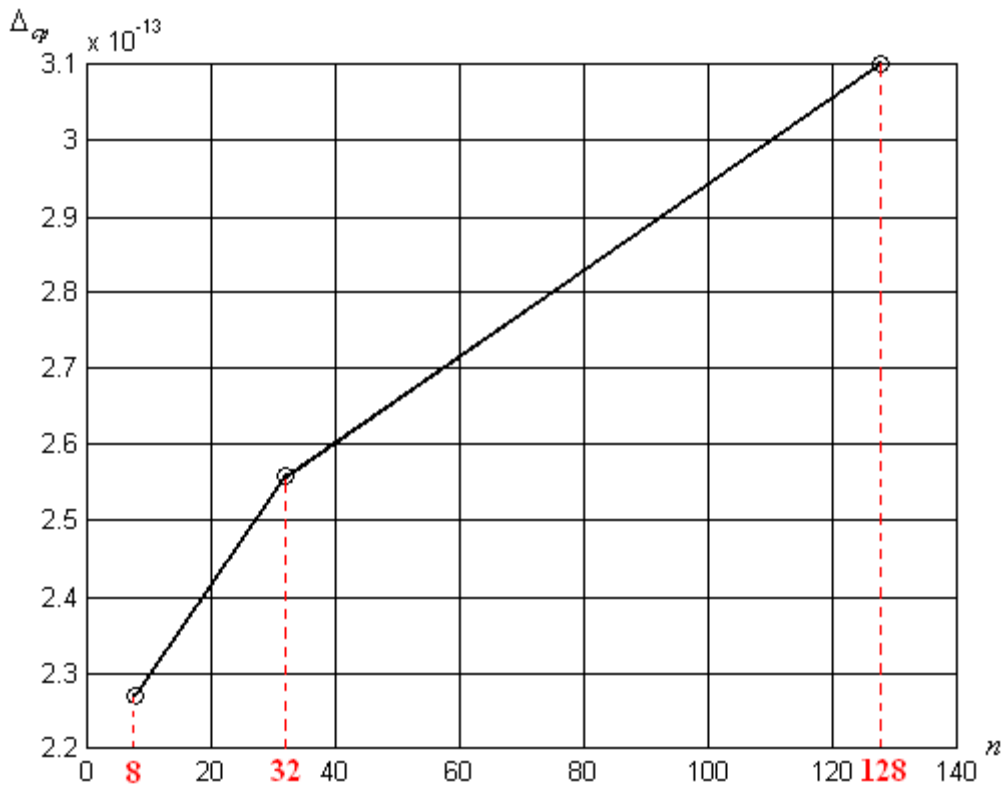
Во множестве действительных чисел последовательное выполнение прямого и обратного ДКП возвращает преобразуемую матрицу к ее первоначальному виду, но в системе чисел с плавающей точкой, допускающей точное представление лишь конечного множества действительных чисел [10], накопление вычислительной погрешности приводит к тому, что результатом обратного ДКП не является исходная матрица. Подтверждением этому явились результаты вычислительного эксперимента, в котором было задействовано 100 ЦИ, хранимых в различных форматах (с потерями, без потерь). В ходе эксперимента матрица каждого ЦИ разбивалась на блоки  $B$  размером  $n \times n$  пикселей. Для каждого блока  $B$  выполнялось прямое (результат –  $B_{DCT}$ ) и обратное дискретное косинусное преобразование (результат –  $B_{DKT}$ ), после чего находилась абсолютная погрешность для каждого элемента матрицы исходного блока путем вычисления  $abs(B_{DKT} - B)$ , где операция вычисления абсолютного значения  $abs(\bullet)$  рассматривается поэлементно. Итогом явилось вычисление среднего значения

погрешности  $\Delta_{cp}$  по всем блокам всех рассмотренных ЦИ для каждого фиксированного  $n$ ,  $n \in \{8, 32, 128\}$ . Результаты эксперимента отражены на рис. 1.

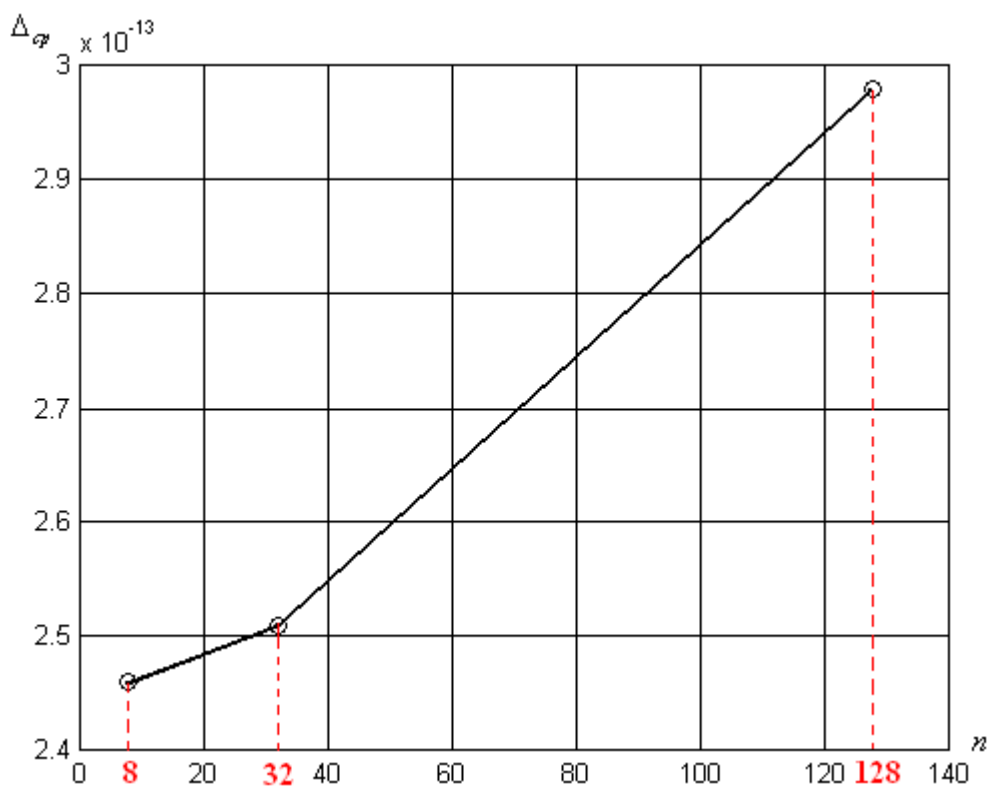
Для ВП аналогичный эксперимент дал результаты, отраженные на рис. 2.

Одной из областей преобразования ЦИ, которая в последнее время используется для организации процесса погружения ДИ, является область сингулярного разложения матрицы/матриц изображения:  $B = U\Sigma V^T$ , где  $U, V$  — ортогональные матрицы левых, правых сингулярных векторов матрицы  $B$  соответственно,  $\Sigma$  — диагональная матрица сингулярных чисел (СНЧ); а также область спектрального разложения матрицы (если эта матрица является симметричной, или приведена к симметричному виду):  $B = U\Lambda U^T$ , где  $U$  — ортогональная матрица собственных векторов (СВ) матрицы  $B$ ,  $\Lambda$  — диагональная матрица собственных значений (СЗ). Стеганопреобразование осуществляется здесь путем модификации СНЧ/СЗ и/или СНВ/СВ. В ходе СП происходит сингулярное/спектральное разложение матрицы блока ЦИ-контейнера, после СП восстанавливается блок  $\bar{B}$  матрицы СС:  $\bar{B} = \bar{U}\bar{\Sigma}\bar{V}^T / \bar{B} = \bar{U}\bar{\Lambda}\bar{U}^T$ , где  $\bar{U}, \bar{\Sigma}, \bar{V}, \bar{\Lambda}$  — результаты определенных модификаций СНВ, СНЧ, СЗ, СВ.

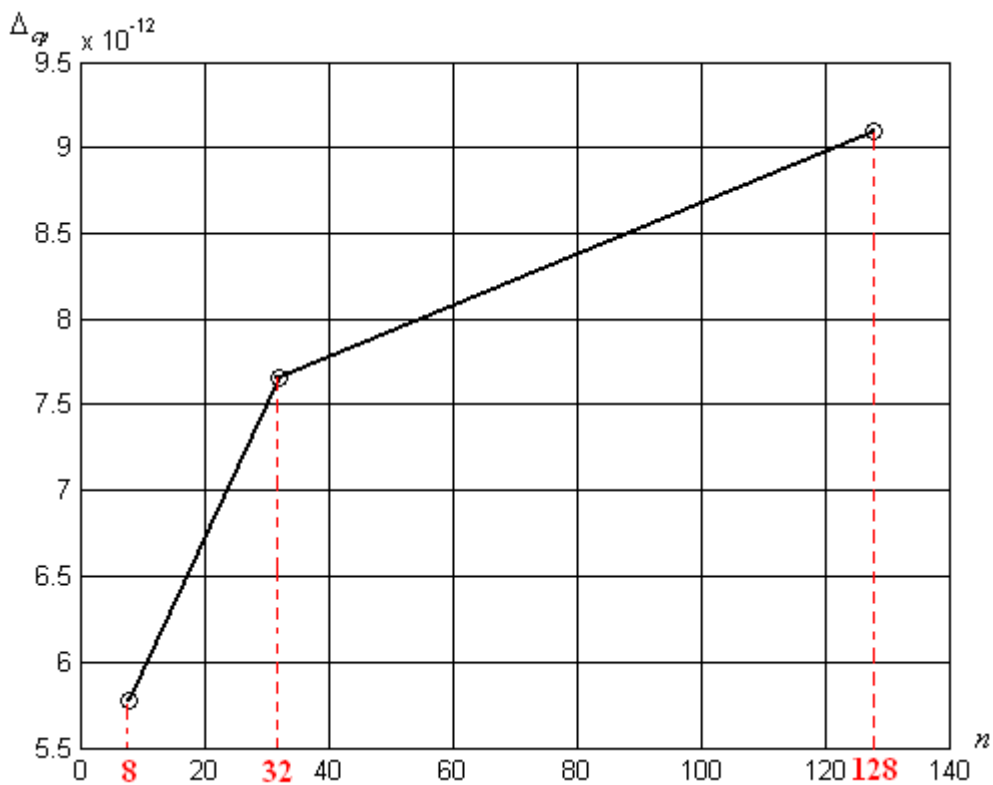
В области действительных чисел при отсутствии какой-либо модификации элементов сингулярных/собственных множителей  $U, \Sigma, V, \Lambda$  матрица  $U\Sigma V^T$  ( $U\Lambda U^T$ ) должна совпасть с матрицей  $B$ , но в системе чисел с плавающей точкой это не происходит из-за накопления вычислительной погрешности. Результаты вычислительного эксперимента для сингулярного разложения матрицы, наглядно иллюстрирующие сделанный вывод, представлены на рис. 3. Аналогичные результаты получены в случае спектрального разложения.



**Рис. 1.** Зависимость средней абсолютной погрешности элементов блока ЦИ при проведении прямого и обратного ДКП от размера блока



**Рис. 2.** Зависимость средней абсолютной погрешности элементов блока ЦИ при проведении прямого и обратного ВП от размера блока



**Рис. 3.** Зависимость средней абсолютной погрешности элементов блока ЦИ при проведении сингулярного разложения от размера блока

Как видно из полученных результатов, абсолютная погрешность элементов восстановленного блока матрицы растет с ростом его размера. Это полностью соответствует ожиданиям: с увеличением размера блока увеличивается количество операций при пересчете его элементов в процессе переходов ПО – ОП, ОП – ПО, происходит накопление погрешности.

Заметим, что абсолютная средняя погрешность элементов матрицы  $B$  при ПО – ОП, ОП – ПО, осуществляемых с использованием сингулярного/спектрального разложения матрицы, на порядок больше, чем с использованием ДКП или ВП.

Несмотря на то, что значения абсолютных погрешностей малы, нельзя забывать о возможности накопления этих погрешностей. Кроме того, их ненулевые значения могут быть увеличены в случае возмущений, которые будут претерпевать элементы области преобразования ЦИ, например, в процессе погружения ДИ, что, как свидетельствуют материалы некоторых публикаций [8], может привести в итоге даже к выходу элементов матрицы ЦИ при возвращении в пространственную область за границы  $[0, 255]$ , что приведет к возникновению погрешности, превосходящей значение погрешности округления, и как следствие, к понижению эффективности декодирования стеганоалгоритма.

## Выводы

В работе для ЦИ с  $m \times m$ -матрицей:

1) Получены оценки вычислительных затрат для проведения переходов ПО – ОП, ОП – ПО, которые составили  $O(m^4)$ ,  $O(m^3)$  операций в случае преобразования всей матрицы,  $O(m^2)$  операций – в случае поблочного преобразования, что при значительных размерах  $m \times m$ -матриц реальных изображений приводят к значительным «накладным» вычислительным затратам;

2) Проведена эмпирическая оценка средней абсолютной погрешности элементов блоков матрицы ЦИ при переходе ПО – ОП, ОП – ПО в случаях наиболее «популярных преобразований»: ДКП, ВП, сингулярного/спектрального разложения матрицы. Установлено, что в условиях машинной арифметики эта погрешность отлична от нуля; погрешность при сингулярном/спектральном разложении на порядок превосходит погрешность при ДКП, ВП, абсолютная погрешность элементов растет с ростом размера обрабатываемого блока матрицы изображения.

В результате проведенных исследований можно сделать вывод, что пространственная область ЦИ-контейнера является предпочтительной по сравнению с областью преобразования контейнера для проведения любых модификаций ее элементов, в частности, для внедрения дополнительной информации, как с точки зрения оценки вычислительной сложности, так с точки зрения оценки вычислительной погрешности.

В настоящий момент усилия автора направлены на разработку устойчивых к возмущающим воздействиям стеганографических алгоритмов, осуществляющих погружение ДИ в пространственной области контейнера. Исходя из [8], существует принципиальная возможность разработки таких алгоритмов, не уступающих по эффективности стеганоалгоритмов, проводящим погружение ДИ в области преобразования.

**Список литературы**

1. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
2. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
3. Bergman, C. Unitary Embedding for Data Hiding with the SVD / C. Bergman, J. Davidson. // Proceedings of Security, Steganography, and Watermarking of Multimedia Contents VII, San Jose, CA, January 17, 2005. — Vol. 5681. — PP. 619–630.
4. Кобозева, А.А. Стеганографический метод, основанный на преобразовании спектра симметричной матрицы / А.А. Кобозева // Праці УНДІРТ. — 2006. — № 4(48). — С. 44–52.
5. Li, C. A novel watermarking scheme for image authentication in DWT domain / C. Li, H. Song // Proceedings of 3<sup>rd</sup> International Conference on Anti-counterfeiting, Security, and Identification in Communication (ASID'09), Hong Kong, 20–22 Aug. 2009. — 2009. — PP. 160–162.
6. Meerwald, P. Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization / P. Meerwald, C. Koidl, A. Uhl // IEEE Transaction on Multimedia. — 2009. — Vol. 11, Iss. 5. — PP. 1037–1041.
7. Кобозева, А.А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации // Искусственный интеллект. — 2007. — № 4. — С. 531–538.
8. Кобозева, А.А. Аналіз захищеності інформаційних систем [Текст] : підруч. для студ. вищ. навч. закл., які навч. за напр. «Інформаційна безпека» та «Системні науки та кібернетика» / А.А. Кобозева, І.О. Мачалін, В.О. Хорошко ; М-во трансп. та зв'язку України, Держ. ун-т інформ.-комунікац. технологій. — К. : ДУІКТ, 2010. — 316 с.
9. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М.: Техносфера, 2006. — 1070 с.
10. Бахвалов, Н.С. Численные методы [Текст] : учебное пособие для студ. физико-математических спец. вузов; Рекомендовано МО РФ / Н.С. Бахвалов, Н.П. Жидков, Г.М. Кобельков. — 6-е изд. — М. : БИНОМ. Лаборатория знаний, 2008. — 636 с.

---

## АНАЛІЗ ПЕРЕВАГ ПРОСТОРОВОЇ ОБЛАСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ-КОНТЕЙНЕРА ДЛЯ СТЕГАНОПЕРЕТВОРЕННЯ

О.В. Костырка

Академія пожежної безпеки імені Героїв Чорнобиля ДСНС України,  
вул. Онопрієнка, 8, Черкаси, 18034, Україна; e-mail: chaykaov@rambler.ru

У роботі проведений детальний аналіз переваг використання для стеганоперетворення просторової області зображення-контейнера в порівнянні з областю перетворення. У ході аналізу отримані оцінки обчислювальної складності переведення зображення із просторової області в області різних перетворень, що найчастіше використовуються у стеганографії, а також оцінки обчислювальної похибки, що виникає в результаті виконання прямого й зворотного перетворення зображення. Встановлено, що просторова область зображення-контейнера є кращою в порівнянні з областю перетворення для вбудови додаткової інформації з погляду оцінки обчислювальної складності й обчислювальної похибки.

**Ключові слова:** цифрове зображення, просторова область, область перетворення зображення, обчислювальна складність, обчислювальна похибка, стеганоперетворення

## ANALYSIS ON THE BENEFITS OF SPATIAL DOMAIN OF COVER IMAGE FOR STEGANOGRAPHY TRANSFORMATION

Olesya V. Kostyrka

Academy of Fire Safety named after Chernobyl Heroes,  
8 Onoprienko str., Cherkassy, 18034, Ukraine; e-mail: chaykaov@rambler.ru

Analysis on the benefits of using spatial domain of cover image for steganography transformation in comparison with steganography transformation domain is discussed. Computational complexities for image transformation from spatial domain to domains of various transformations are defined. We obtain estimates of the computational error of the image transformation. We have shown that spatial domain of cover image is preferable for embedding additional information than steganography transformation area.

**Keywords:** digital image, spatial domain, image processing transform domain, computational complexity, computational error, steganography transformation

# SYNCHRONIZATION SIGNALS IN PACKET SWITCHED NETWORKS: PARAMETER MONITORING AND MEASUREMENT

Nataliya V. Fedorova

State University of Telecommunications,  
7 Solomenskaya str., Kyiv, 03680, Ukraine; e-mail: Natasha\_f@ukr.net

In the present paper, measurement of the parameters of synchronization signals in IP/MPLS transport networks is considered. The results of measurements of synchronization signal instability indices for base station are presented. The basic principles for the development of the system for monitoring synchronization signals are considered.

**Keywords:** packet switched network (IP/MPLS network), synchronization signal, parameters of synchronization signals, measurement of the parameters of synchronization signals, monitoring of synchronization signals

## Introduction

Because synchronization issues are crucial for modern IP/MPLS transport networks [1–4], enhancement of the role of synchronization network is the modern trend in the development of primary network, and this trend will continue in the immediate future [2]. Moreover, synchronization problems are related not only to primary network, but are important when developing access networks with consideration for various technologies and protocols embodied in the specific IP/MPLS network [2–4].

Measurement of parameters of reference signals as well as evaluation of their instability is a prerequisite for the solution of synchronization problems in electric communication networks.

The *aim* of the paper is to solve the following topical issue: measuring the parameters of synchronization network in IP/MPLS network, and real-time monitoring of these indices to provide for timely response to network emergencies.

## Problem statement

Currently, in communication operator networks, more and more network segments are being deployed for communicating through IP/MPLS transport only. However, with increase in the number of devices (e.g., mobile communication base stations), synchronization problems should be considered on a systemic level rather than on case-by-case basis. To this is related some kind of local revolution in approach: arrival of some «critical mass» of users of synchronization signals in the IP/MPLS network results in the requirement for considering synchronization system as a separate component of electric communication system.

With the following increase in the number of digital devices, the concepts of the development and principles of control of synchronization network start being subjected to changes. Such system-based approach may be provided by measurement of the parameters of synchronization network.

Therefore, this work is devoted to the solution of the following topical problems:

- 1) Measuring the parameters of synchronization network in IP/MPLS network, and
- 2) Real-time monitoring of these indices.

## Main part

In «Definition and Terminology for Synchronization Networks» [1], TIE (Time Interval Error), MTIE (Maximum Time Interval Error) and TDEV (Time Deviation) are the three parameters used as basic criteria for evaluation of quality of synchronization signals, but only TIE function is directly measured.

TIE is defined as the time deviation between the signal being measured and the reference clock. One can perform calculation of MTIE based on obtained TIE array.

MTIE is defined as the maximum peak-to-peak delay variation of a given synchronization signal with respect to an ideal synchronization signal within an observation time for all observation times of that length within the measurement period. Besides, performed is the calculation of TDEV (Time Deviation), which is described as «a measure of the expected time variation of a signal as a function of integration time» [1]. TDEV may provide information on spectral components of either phase or time noise of the signal.

Because, by definition, MTIE equals peak-to-peak delay variation of a given synchronization signal with respect to an ideal synchronization signal within a certain period, it provides for the detection of phase transients in synchronization signal. However, because of its sensitivity to phase transients, MTIE is inadequate to show the underlying noise of synchronization signal.

Random noise is better characterized by TDEV which is an RMS power estimator instead of a peak estimator. TDEV tends to remove transients in a synchronization signal, and is therefore a better estimator of the underlying noise processes [2]. It has been shown [5] that measurements may be taken at digital ports of terminal equipment (at Tributary E1) and directly at Ethernet port (for this purpose, such special meters as STA-61 (Spectracom) and Paragon-m (Oscilloquartz) have been developed recently).

## Measurement Example

Measurements of frequency stability parameters were performed in IP/MPLS network at the level of PE-router with three retransmissions for synchronization of mobile communication base station connected through IP. As the reference frequency for IP/MPLS network, use was made of a clock net signal transmitted through SDH (Synchronous Digital Hierarchy) network. Sources of clock signal were cesium oscillators and GPS-receivers distributed over the network. From PE Level, the signal can be distributed to the lower levels (e.g., to P Level), and, correspondingly, can be used for synchronization of the base unit.

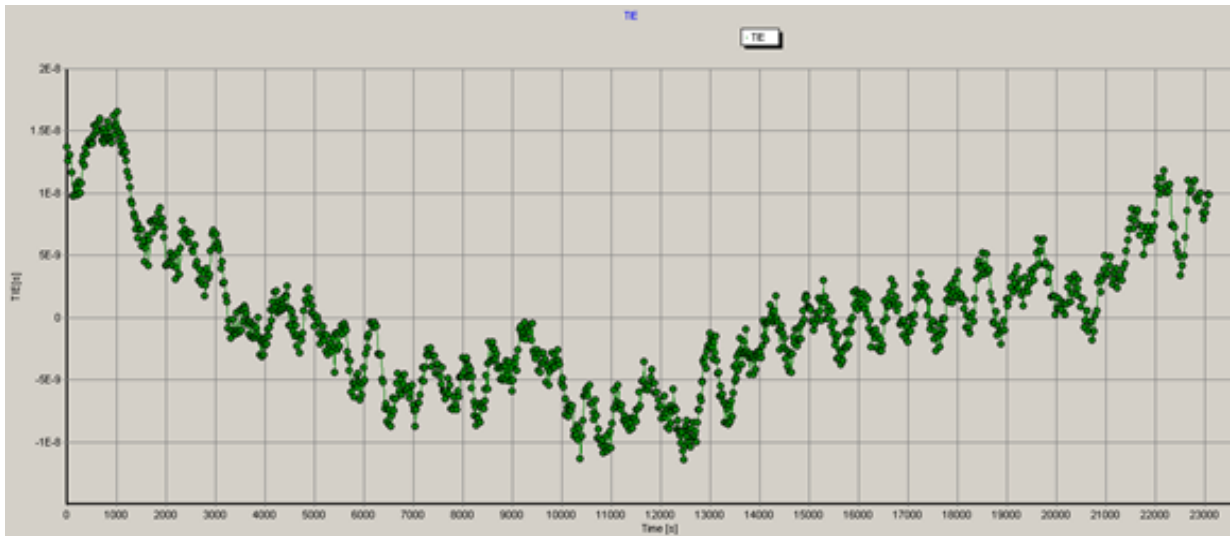
MTIE and TDEV mask in accordance with the ITU-T Requirements G.811 (timing requirements of primary reference clocks) is shown in Figs. 1(b) and 1(c), respectively. MTIE and TDEV were calculated based on directly obtained TIE values (see Fig. 1(a)).

The signal is suitable for a base station, because its daily stability is better than  $5 \times 10^{-8}$ .

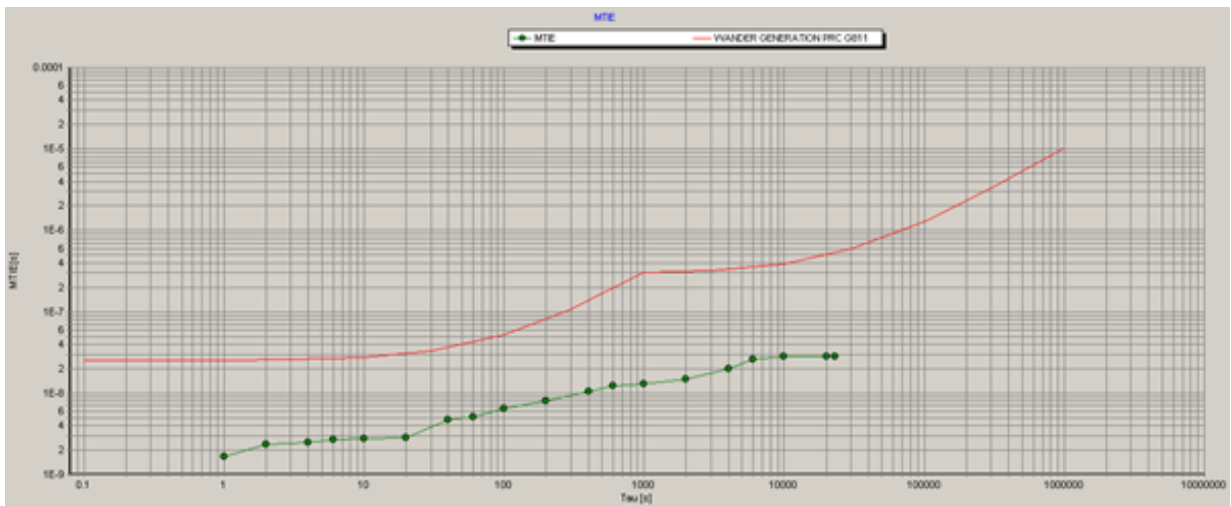
Strictly speaking, there is no requirement for synchronization as such for network core and aggregation level. However, when implementing an IP/MPLS network and performing station-by-station deployment of a great number of base stations with IP interfaces in large networks, a problem related to synchronization between old base stations and remaining islands of conventional TDM (Time Division Multiplexing) transport network may occur. Therefore, there may take place a transfer of synchronization signal from IP/MPLS cloud to separate SDH sections, and directly to base stations themselves through organization of separate E1 streams. Interestingly, that, in such a case, traffic and signal data may be transferred in a similar way to (1) minimize time and cost when implementing transfer to



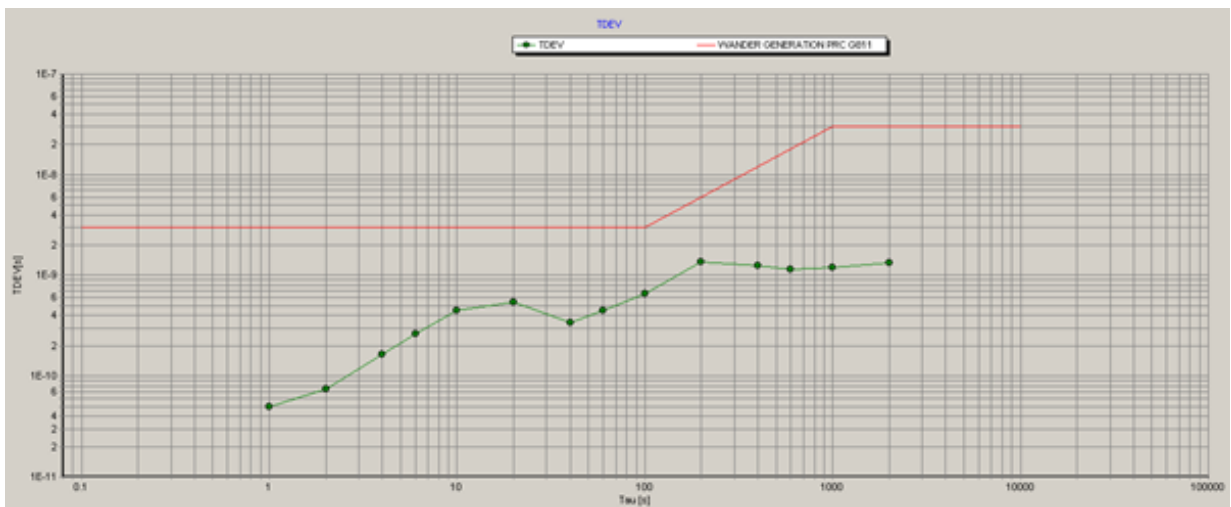
packet networks and (2) make the very process of upgrade (or change) of base stations for those with IP interface more flexible.



a



b



c

**Fig. 1.** Measurements of stability parameters: a — time interval error (TIE); b — Maximum Time Interval Error (MTIE) and c — Time Deviation (TDEV)

When deploying and operating a synchronization network within IP/MPLS transport network, it becomes necessary to develop a synchronization signal monitoring system. The latter system must depend neither on the number of equipment manufacturers nor on the number of sources of synchronization signal. It is proposed to perform continuous measurement of TIE values for the signals from several primary sources with respect to each other, and, based on gradually accumulated data, to calculate MTIE and TDEV values at predetermined time intervals.

The number of signals to be compared should be at least three; it will provide for identification of abnormal signal based on majority decision. For this purpose, software-and-hardware complexes are developed to become the backbone of monitoring system. In this case, the meters may be represented by the above-mentioned state-of-the-art measurement devices to be installed stationary within the network.

Unlike synchronization of classic digital networks, the measurement points within IP/MPLS networks may be of more variable locations due to flexibility of IP-based configuration [3, 4].

Therefore, based on continuous monitoring, it is possible to decide which of the three signals is out of the norms defined by the masks of ITU-T requirement G.811. To calculate MTIE and TDEV values, firstly, TIE data arrays accumulated; then, the results will be produced at definite time intervals.

Another parameter used to assess synchronization quality should be mentioned. Packet Delay Variation (PDV) characterizes IP/MPLS network load level depending on packet delay. In classic digital networks, this parameter is absent because of the very nature of these networks. PDV value should not exceed 50 ms; otherwise, synchronization signal stability parameters will be out of the norms defined by the masks of ITU-T requirement G.811 [2]. This fact has been confirmed by MTIE and TDEV measurements at the pilot section of synchronization network in IP/MPLS network.

PDV parameter is measured with special meters STA-61 (Spectracom) and Paragon-m (Oscilloquartz) and may represent an operating parameter in the synchronization network monitoring system being developed for IP/MPLS transport network.

## Conclusions

In the present work, the following conclusions and results were obtained:

1) With increase in the number of devices, synchronization problems should be considered on a systemic level rather than case-by-case basis, i.e., arrival of some “critical mass” of users of synchronization signals in the IP/MPLS network results in the requirement for considering synchronization system as a separate component of electric communication system.

2) With increase in the number of digital devices, the concepts of the development and principles of control of synchronization network start being subjected to changes. Such system-based approach may be provided by measurement of the parameters of synchronization network.

3) TIE, MTIE and TDEV are the three parameters used as basic criteria for evaluation of performance of synchronization signals. This work presents the results of practical measurements. Besides, there has been established a relationship between synchronization quality and network load level using PDV index.

4) In this paper, we addressed the issues of the development of synchronization network monitoring system in IP/MPLS transport network. This system must depend neither on the number of equipment manufacturers nor on the number of sources of synchronization signal. A full-blown monitoring system, if available, will provide for timely response to network emergencies.

## References

1. Рекомендация ITU-T G.810 «Терминология сетей синхронизации»
2. Mills, D.L. Computer Network Time Synchronization : the Network Time Protocol / D.L. Mills. — Boca Raton, FL : CRC/Taylor & Francis, 2006. — 286 p.
3. Вакась, В.И. Синхронизация базовых станций при внедрении технологий IP-сетей / В.И. Вакась, И.П. Черняк // Материалы 21-й Международной крымской конференции «СВЧ-техника и телекоммуникационные технологии» (КрыМиКо'2011), 12–16 сент. 2011 г., Севастополь. — Севастополь: Вебер, 2011. — С. 374–375.
4. Вакась, В.И. Комбинирование методов обеспечения синхронизацией базовых станций от разных иерархических уровней сети с коммутацией пакетов / В.И. Вакась, Н.В. Федорова // Материалы 22-й Международной крымской конференции «СВЧ-техника и телекоммуникационные технологии» (КрыМиКо'2012), 10–14 сент. 2012 г., Севастополь. — Севастополь: Вебер, 2012. — С. 320–321.
5. Вакась, В.И. Практические аспекты синхронизации сетей IP/MPLS [Текст] / В.И. Вакась, Н.В. Федорова // Зв'язок. — 2013. — № 1. — С. 23–27.

### СИГНАЛИ СИНХРОНІЗАЦІЇ У МЕРЕЖАХ З КОМУТАЦІЄЮ ПАКЕТІВ. КОНТРОЛЬ І ВИМІР ЇХ ПАРАМЕТРІВ

Н.В. Федорова

Державний університет телекомунікацій,  
вул. Солом'янська, 7, Київ, 03680, Україна; e-mail: Natasha\_f@ukr.net

Розглянуто проведення вимірювань параметрів сигналів синхронізації в транспортних мережах IP/MPLS. Представлені результати вимірювань показників нестабільності сигналу синхронізації для базової станції. Розглянуто основні принципи створення системи моніторингу для сигналів синхронізації.

**Ключові слова:** мережа з комутацією пакетів (мережа IP/MPLS), сигнал синхронізації, параметри сигналу синхронізації, вимірювання параметрів сигналу синхронізації, моніторинг сигналу синхронізації

### СИГНАЛЫ СИНХРОНИЗАЦИИ В СЕТЯХ С КОММУТАЦИЕЙ ПАКЕТОВ. КОНТРОЛЬ И ИЗМЕРЕНИЕ ИХ ПАРАМЕТРОВ

Н.В. Федорова

Государственный университет телекоммуникаций,  
ул. Соломенская, 7, Киев, 03680, Украина; e-mail: Natasha\_f@ukr.net

Рассмотрено проведение измерений параметров сигналов синхронизации в транспортных сетях IP/MPLS. Представлены результаты измерений показателей нестабильности сигнала синхронизации для базовой станции. Рассмотрены основные принципы создания системы мониторинга для сигналов синхронизации.

**Ключевые слова:** сеть с коммутацией пакетов (сеть IP/MPLS), сигнал синхронизации, параметры сигнала синхронизации, измерение параметров сигнала синхронизации, мониторинг сигнала синхронизации

# ІНТЕРАКТИВНІ КОМУНІКАТИВНІ ТЕХНОЛОГІЇ ОСВІТИ: МОБІЛЬНЕ НАВЧАННЯ ЯК НОВА ТЕХНОЛОГІЯ В ПІДВИЩЕННІ МОВНОЇ КОМПЕТЕНЦІЇ СТУДЕНТІВ НЕМОВНИХ ВНЗ

О.В. Мардаренко

Одеський національний політехнічний університет,  
просп. Шевченка, 1, Одеса, 65044, Україна

Виконано аналіз основних засад та напрямів використання мобільних технологій у навчанні іноземних мов у немовних ВНЗ. Відзначається, що сучасні засоби мобільної комунікації являють собою значний потенціал для підвищення професійної і мовної компетенції студентів немовних ВНЗ. Розглянуто головну проблему ефективного використання мобільних засобів інтерактивних комунікативних технологій (ІКТ) у викладанні іноземних мов. Дано рекомендації і спрощена технологія (методика) використання мобільних пристроїв у навчанні для підвищення мовної компетенції.

**Ключові слова:** мобільне навчання, мобільні технології, інтерактивні технології, навчання мов.

## Вступ

Сучасні комунікатори (смартфони, КПК, камерфони, айфони, планшети тощо) надають їх власникам такі функціональні можливості як: робота в стільникових мережах різних стандартів з виходом в Інтернет; підтримка знімних носіїв інформації (ємність таких носіїв перевищує 4-8 ГБ); підтримка кольорових дисплеїв (320x240, 640x200, 640x480 і більше); потужні мобільні процесори; велика тривалість роботи без перезарядки; зручний форм-фактор.

Не важко помітити, що цих можливостей цілком достатньо для повноцінної мобільної роботи в різних професійних сферах – бізнесі, науці та освіті. Особливо цікавим і перспективним є використання сучасних мобільних пристроїв в напрямку технологій дистанційного навчання, як мобільного навчання. Головна проблема з якою сьогодні стикаються викладачі – це ефективне використання засобів ІКТ у викладанні іноземних мов.

Основна мета навчання студентів немовного вищого закладу освіти полягає у формуванні професійної компетенції спеціаліста за своїм фахом. Як відомо професійна компетенція складається з двох частин: професійної комунікативної компетенції та іншомовної комунікативної компетенції. У методиці навчання іноземних мов вагома роль для організації ефективного формування складових комунікативної компетенції відводиться апаратним (технічним) засобам.

Серед існуючих в освітніх закладах технічних засобів найбільш широко використовуються комп'ютери з мультимедійними програмами, спеціальне лінгафонне обладнання, відео та інше. Але сучасні наукові досягнення на практиці досить часто застосовуються не повною мірою. Багато вищих закладів освіти ще недостатньо забезпечені такими технічними засобами як лінгафонне обладнання, відео- та комп'ютерні класи тощо. Одна з причин – обладнання і програми дорого коштують. Не

кращий стан і з дидактичним забезпеченням. Закладам освіти бракує відеокурсів і мультимедійних комп'ютерних програм. А при їх наявності вони недостатньо забезпечені методичними розробками, що знижує ефективність їх застосування у процесі навчання іноземних мов.

*Метою* статті є аналіз публікацій з мобільних технологій навчання та розробка пропозицій до методики застосування технічних (апаратних) засобів у мобільному навчанні в контексті вивчення іноземних мов.

## Основна частина

Проблема використання технічних засобів і дидактичних матеріалів у навчанні не є новою, питання використання стільникових функцій мобільних пристроїв у навчальному процесі виникло ще у 80-х роках 20-го сторіччя. З розвитком мобільних технологій зростає потреба і можливість швидкого доступу до інформації і особливо іншомовної, адже зростає мобільність населення і потужність мобільних пристроїв. Тому особливої актуальності набуває пошук нових підходів до організації навчального процесу і створення навчальних матеріалів і технологій, які б враховували можливості мобільних пристроїв.

Під мобільними інформаційно-комунікативними технологіями будемо розуміти сукупність персональних апаратних засобів, програмного забезпечення, а також прийомів, засобів і методів, що дозволяють здійснювати діяльність, пов'язану з отриманням, збереженням, комп'ютерним опрацюванням і відтворенням текстових, аудіо-, відео- та графічних даних в умовах оперативної комунікації з ресурсами Інтернету, що спрямовані на підтримку особистісно-орієнтованого навчання [1].

За останні 5 років були широкі дебати про те, як визначити саме те, що є мобільним навчанням. Труднощі в досягненні консенсусу пов'язані частково з швидким розвитком мобільного навчання. Європейська гільдія з електронного навчання визначає його так: будь-яка діяльність, яка дозволяє людям бути більш продуктивними у споживанні, взаємодії або створенні інформації компактними цифровими пристроями, якщо людина призводить ці дії на регулярній основі, має надійний зв'язок і пристрій поміщається в кишені або сумочці [2].

Отже, термін «мобільне навчання» (м-навчання), або *mobile learning (m-learning)*, відноситься до використання у викладанні та навчанні мобільних і портативних ІТ-пристроїв, таких, як кишенькові комп'ютери PDA (Personal Digital Assistants), мобільні телефони, ноутбуки, нетбуки, планшетні ПК, *iPhone*, *iPad* та інше.

Мобільний Assisted Learning. Мова (MALL) – технологія навчання мовам за допомогою портативних мобільних пристроїв, таких як мобільні телефони (стільникові телефони), MP3- і MP4-плеєри, КПК, *iPhone* або *iPad* та інше. MALL є підмножиною мобільного навчання (м-навчання) і комп'ютерного навчання мовам (CALL) [3].

Огляд і аналіз публікацій з мобільного навчання свідчить, що сучасні мобільні пристрої в розвинутих країнах використовуються в галузі освіти, управління, організації викладання для фахівців-практиків, а також як технічні засоби підтримки навчання для учнів та студентів. Зростання їх використання почалося з початку 21-го століття в різних сферах суспільного життя, як реакція на задоволення потреб людей у русі [4]. Особливо увага до мобільного навчання зростає у вищих навчальних закладах про що свідчать зростання наукових публікацій і зарубіжних наукових конференцій (наприклад, *mLearn*, *IMCL*), зростання кількості наукових журналів, технічних звітів і книг (Тракслер, 2008; Herrington & Herrington, 2008; Kukulska-Хьюм і Тракслер, 2005; Ally, 2009) [5–8]. Інтернет, як ресурс, може збагатити і розширити можливості вивчення мови. Ця додаткова функціональність Web буде підтримувати створення інтерактивних веб-сторінок для мовної практики [9].

Зарубіжні і українські науковці в своїх публікаціях [10–13] констатують такі основні переваги мобільних технологій в порівнянні з комп'ютерними: учні можуть взаємодіяти один з одним і з викладачем; набагато простіше розмістити в класі кілька мобільних пристроїв, ніж кілька настільних комп'ютерів; кишенькові або планшетний ПК (КПК) і електронні книги легше і займають менше місця, ніж підручники з паперу і навіть ноутбуки; розпізнавання за допомогою стилуса або сенсорного екрану стає більш наочним, ніж при використанні клавіатури і миші; існує можливість обміну завданнями та спільної роботи; учні та викладачі можуть надсилати текст по електронній пошті, вирізати, копіювати і вставляти, передавати пристрої всередині групи, працювати один з одним, використовуючи інфрачервоні функції КПК або бездротової мережі, наприклад, Wi-Fi або Bluetooth; мобільні пристрої можуть бути використані в будь-якому місці, в будь-який час, в тому числі у будинку, в поїзді, в готелях, в аудиторії чи за місцем роботи; нові технічні пристрої, такі, як мобільні телефони, гаджети, ігрові пристрої тощо, залучають учнів – молодих людей, які, можливо, втратили інтерес до освіти; м-навчання (m-learning) через мобільний пристрій робить навчання дійсно індивідуальним. Учні мають можливість вибору змісту навчання з урахуванням їх інтересів, в результаті чого m-learning є орієнтований на студента. Гнучкість та негайний доступ до інформації, необхідної для конкретної роботи, дозволяє за допомогою мобільних пристроїв підвищити продуктивність праці людини; самостійне навчання і негайне надання контенту за запитом є характерними рисами m-learning, надає користувачам можливість пройти навчання в поза робочий час і створює умови для спільного навчання та взаємодії.

Останніми тенденціями в навчанні є змішане навчання, яке поєднує в собі різні види навчання, щоб зробити навчання більш ефективним і цікавим. Змішане навчання поєднує в собі переваги різних форм навчання, і краще всього підходить до контексту навчання в інтерактивному навчальному середовищі. Мобільне навчання можна комбінувати з іншими видами навчання, забезпечуючи інтерактивні умови навчання для студентів.

Засоби мобільних ІКТ навчання можна розділити на апаратні і програмні. Існуючі програмні мобільні засоби навчання, або програмні мобільні системи підтримки навчання МСПН: *MLE-Moodle*, *Blackboard*, *Mobile ELDIT*, *Amadeus LMS Mobile*, *Hot Lava Mobile* (HLM), *SumTotal ToolBook*, *Lectora*, *MLEX*, *MoSync*, *MentorMate*, *OnPoint Digital*, *mobiSiteGalore*, *LearnCast*, *Clickatell*, *Mobl21* та інші досліджувались Рашевською Н.В. [14]. В зв'язку з цим фрагментарно розглянемо тільки дві програмні платформи, які розроблені спеціально з метою навчання мов а більш детально розглянемо сучасні апаратні мобільні засоби і їх функціональні можливості.

Отже, платформа *Mobile ELDIT* – мобільна система підтримки навчання, що розроблена в Італії з метою підтримки процесу навчання мов. МСПН *Mobile ELDIT* складається із словника, набору текстів і тестових завдань. Схожою МСПН для створення навчальних матеріалів для вивчення мов є система *MobiLearn*.

Інша, платформа *Mobl21* є платформою для мобільного навчання, яку можуть використовувати як викладачі для створення навчальних матеріалів, так і студенти для створення конспектів занять. За допомогою *Mobl21* можна: швидко й ефективно створювати навчальні матеріали у вигляді мультимедійних навчальних посібників; студенти можуть отримати доступ до матеріалів у зручний для них час і в будь-якому місці; студенти можуть переглядати матеріал у зручному для них темпі; викладач може керувати змістом і користувачами системи підтримки навчання; студенти можуть проходити тестування і брати участь у вікторинах.

Всі сучасні апаратні пристрої, на які встановлені вказані в табл. 1 операційні системи, безкоштовно підтримують мовні функціональні можливості без додаткового програмного забезпечення.

Таблиця 1.

Сучасні мобільні операційні системи пристроїв і можливості платформ

| Можливості/платформа                    | Android | BlackBerry | iPhone | Nokia S60 | Windows CE |
|---|---------|------------|--------|-----------|------------|
| Переклад з різних мов                   | так     | так        | так    | так       | так        |
| Має мовні словники                      | так     | так        | так    | так       | так        |
| Читає іноземні скрипти                  | так     | ні         | так    | так       | так        |
| Перетворює текст в мову                 | так     | ні         | так    | ні        | ні         |
| Має голосовий набір                     | так     | ні         | так    | ні        | ні         |
| Зберігає історію                        | так     | ні         | так    | так       | так        |
| Можливі розмови в інтерактивному режимі | так     | ні         | ні     | ні        | ні         |

Під функціональними можливостями ми розуміємо сервіси, що пропонують ОС і сам пристрій своїм користувачам: переклад слів, фраз, абзаців або повного тексту; кількість мов і напрямків перекладу; можливість аудіювання слів, фраз, тексту; тип інтерфейсу вводу – текстовий або звуковий та інше. Спільними характеристиками таких систем є те, що на платформи зазначених ОС можливо встановити безкоштовні додатки: браузер *Google Chrome* і програму *Google Translate*.

У навчанні іноземних мов провідним методичним принципом, є принцип комунікативності, що передбачає побудову процесу навчання як моделі процесу реальної комунікації. Комунікація – це процес обміну інформацією (фактами, ідеями, поглядами, емоціями тощо) між індивідами, що спілкуються. Комунікативні ситуації, що використовуються в навчанні іноземних мов, мають відтворювати типові ситуації реального життя у відповідній сфері спілкування. Важливим фактором, що впливає на процес комунікації, є організація взаємодії (діалогу) між індивідами, що спілкуються, а саме інтерактивна функція комунікації (обмін діями) [1, 14].

Функцію інтерактивного співрозмовника-користувача, наприклад, можна покласти на програму *Google Translate*, браузер та комутативні можливості операційних систем і електронних пристроїв. *Google Translate* – безкоштовний додаток, який можна встановити на всі вказані пристрої.

Браузер *Google Chrome*, встановлений на мобільних пристроях OS *Android*, має можливості доступу до додатків *Google Play* на 30 мовах і йому додані нові функції, в тому числі: користувач може запитати настільну версію веб-сайту, у випадку, якщо він не хоче переглядати мобільну версію; додавати закладки для швидкого доступу на робочому столі, що забезпечує більш швидкий перехід на улюблені сайти; вибрати свої улюблені програми для обробки посилань відкритих в *Chrome*. Програма *Android* має налаштування проксі для Wi-Fi доступу. Є можливість використовувати *Chrome* з системою проксі в настройках *Android* і підключатись до Інтернету по Wi-Fi мережі [15].

Оскільки комп'ютери та Інтернет стали необхідними освітніми інструментами і з'явилися більш портативні та доступні, більш ефективні і прості у використанні пристрої, відкриваються великі можливості для розширення участі та доступу до ІКТ, зокрема в Інтернеті. Мобільні пристрої мають більш «розумні» ціни, ніж настільні комп'ютери, і є більш дешевим засобом доступу до Інтернету. Якщо взяти до уваги сучасні процесорні потужності мобільних пристроїв, планшетних і карманних ПК то слід відзначити, що з'явилась можливість використовувати мобільний доступ в Інтернет з однаковою функціональністю з настільними комп'ютерами.

Застосування технічних засобів у процесі навчання іноземних мов дає можливість: створення природного мовленнєвого середовища як вагомого чинника у

навчанні іноземних мов; підвищення зацікавленості студентів у вивченні іноземних мов; використання диференційованого підходу до навчання; здійснення інтенсифікації навчального процесу.

Ефективність використання апаратних засобів визначається, головним чином, за такими аспектами: параметрами й можливостями апаратних засобів та їх використанням у конкретних умовах; якістю дидактичного матеріалу; вміннями викладача й студентів використовувати апаратні засоби і дидактичні матеріали.

Невизначеність щодо авторських прав на електронні дані може утруднити формування інформації придатної для відтворення з мобільних пристроїв. Розробка мобільних додатків вимагатиме підвищення кваліфікації викладачів або залучення фахівців. Природно, що для цього знадобиться спеціальне програмне забезпечення, яке б могло використовуватися на різних платформах комунікаторів.

## Висновок

Розглянуто методологічні, організаційні і технічні (апаратні) аспекти побудови та застосування інтерактивних комунікативних технологій освіти, які орієнтовано на процес вивчення іноземних мов. Дано тлумачення основних визначень ІТК, їх структуру, а також рекомендації щодо використання мобільних пристроїв у навчанні для підвищення мовної компетенції.

## Список літератури

1. Коваль, Т.І. Інтерактивні технології навчання іноземних мов у вищих навчальних закладах [Електронний ресурс] / Т.І. Коваль // Інформаційні технології і засоби навчання. — 2011. — № 6(26). — Режим доступу: <http://journal.iitta.gov.ua/index.php/itlt/article/view/546/451> (Дата звернення: 26.08.2013).
2. What is m-learning? [Електронний ресурс] // Tribal's Digital Learning Studio. Cambridge, United Kingdom. Режим доступу: <http://www.m-learning.org/knowledge-centre/whatismllearning> (Дата звернення: 26.08.2013).
3. Mobile Assisted Language Learning (MALL) [Електронний ресурс] // Wikipedia. The Free Encyclopedia. Wikimedia Foundation, Inc. Режим доступу: [http://en.wikipedia.org/wiki/Mobile\\_Assisted\\_Language\\_Learning](http://en.wikipedia.org/wiki/Mobile_Assisted_Language_Learning) (Дата звернення: 26.08.2013).
4. Crow, R. Switching Gears: Moving from e-Learning to m-Learning [Електронний ресурс] / R. Crow, et al. // MERLOT Journal of Online Learning and Teaching. — 2010. — Vol. 6, No. 1. — Режим доступу: [http://jolt.merlot.org/vol6no1/crow\\_0310.htm](http://jolt.merlot.org/vol6no1/crow_0310.htm) (Дата звернення: 26.08.2013).
5. Ally, M. Mobile Learning: Transforming the Delivery of Education and Training / M. Ally. — Athabasca, AB: Athabasca University Press, 2009. — 297 p.
6. The First IEEE International Workshop on Wireless and Mobile Technologies in Education (WMTE 2002) [Електронний ресурс] // IEEE Technical Committee on Learning Technology. Kaohsiung, Taiwan. Режим доступу: <http://lttf.ieee.org/wmte2002/> (Дата звернення: 26.08.2013).
7. Second IEEE International Workshop on Wireless and Mobile Technologies in Education (WMTE 2002) [Електронний ресурс] // IEEE Technical Committee on Learning Technology. Kaohsiung, Taiwan. Режим доступу: <http://lttf.ieee.org/wmte2004/> (Дата звернення: 26.08.2013).
8. Caudill, J. The Growth of m-Learning and the Growth of Mobile Computing: Parallel developments [Електронний ресурс] / J. Caudill // The International Review of Research in Open and Distance Learning. — 2008. — Vol. 8, No. 2. — Режим доступу: <http://www.irrodl.org/index.php/irrodl/article/view/348/873> (Дата звернення: 26.08.2013).
9. Brandl, K. Integrating internet-based reading materials into the foreign language curriculum: from teacher- to student-centered approaches / K. Brandl // Language Learning & Technology. — 2002. — Vol. 6, No. 3. — PP. 87–107.
10. Valarmathi, K.E. Mobile Assisted Language Learning [Електронний ресурс] / K.E. Valarmathi // Journal of Technology for ELT. — 2011. — Vol. II, No. 2. — Режим доступу: <https://sites.google.com/site/journaloftechnologyforelt/archive/april2011/mobileassistedlanguagelearning> (Дата звернення: 26.08.2013).



11. VII Міжнародна науково-практична конференція «Сучасні підходи та інноваційні тенденції у викладанні іноземних мов» [Електронний ресурс] / Кафедра англійської мови технічного спрямування №2. НТУУ КПІ. Київ, Україна. Режим доступу: <http://kamts2.kpi.ua/node/383> (Дата звернення: 26.08.2013).
12. Бугайчук, К.Л. Мобільне навчання: сутність і моделі впровадження в навчальний процес вищих навчальних закладів МВС України [Електронний ресурс] / К.Л. Бугайчук // Інформаційні технології і засоби навчання. — 2012. — № 1(27). — Режим доступу: <http://journal.iitta.gov.ua/index.php/itlt/article/view/619/480> (Дата звернення: 26.08.2013).
13. Куклев, В.А. Становление системы мобильного обучения в открытом дистанционном образовании : автореф. дис. на соискание уч. степени доктора пед. наук : спец. 13.00.01 «Общая педагогика, история педагогики и образования» / В. А. Куклев ; Ульяновский государственный технический университет. — Ульяновск, 2010. — 46 с.
14. Рашевська, Н.В. Програмні засоби мобільного навчання [Електронний ресурс] / Н.В. Рашевська // Інформаційні технології і засоби навчання. — 2011. — № 1(21). — Режим доступу: <http://journal.iitta.gov.ua/index.php/itlt/article/view/369/353> (Дата звернення: 26.08.2013).
15. Chrome for Android Update [Електронний ресурс] // Google Chrome Blog. The latest news from the Google Chrome team. Режим доступу: <http://chrome.blogspot.com/2012/04/chrome-for-android-update.html> (Дата звернення: 26.08.2013).

### ИНТЕРАКТИВНЫЕ КОММУНИКАТИВНЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ: МОБИЛЬНОЕ ОБУЧЕНИЕ КАК НОВАЯ ТЕХНОЛОГИЯ В ПОВЫШЕНИИ ЯЗЫКОВОЙ КОМПЕТЕНЦИИ СТУДЕНТОВ НЕЯЗЫКОВЫХ ВУЗОВ

Е.В. Мардаренко

Одесский национальный политехнический университет,  
просп. Шевченко, 1, Одесса, 65044, Украина

Выполнен анализ основных принципов и направлений использования мобильных технологий в обучении иностранным языкам в неязыковых ВУЗах. Отмечается, что современные средства мобильной коммуникации представляют собой значительный потенциал для повышения профессиональной и языковой компетенции студентов неязыковых ВУЗов. Рассмотрена проблема эффективного использования мобильных средств интерактивных коммуникативных технологий (ИКТ) в преподавании иностранных языков. Даны рекомендации и упрощенная технология (методика) использования мобильных устройств в обучении для повышения языковой компетенции.

**Ключевые слова:** мобильное обучение, мобильные технологии, интерактивные технологии, обучение иностранным языкам

### INTERACTIVE COMMUNICATION TECHNOLOGIES IN EDUCATION: MOBILE LEARNING AS A NEW TECHNOLOGY OF IMPROVING OF LANGUAGE COMPETENCE OF NON-LINGUISTIC UNIVERSITY STUDENTS

Elena V. Mardarenko

Odessa National Polytechnic University,  
1 Shevchenko Ave., Odessa, 65044, Ukraine

The analysis of basic principles and directions of the use of mobile technologies is executed in educating to the foreign languages in non-linguistic institutions of higher learning. It is marked that modern facilities of mobile communication are considerable potential for the increase of professional and language competence of students of non-linguistic institutions of higher learning. The problem of the effective use of mobile facilities of interactive communicative technologies is considered in teaching of foreign languages. Recommendations and simplified methodology of the use of mobile devices are given in educating for the increase of language competence.

**Key words:** mobile learning, mobile technologies, interactive technologies, foreign language

**ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ**

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

**ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ**

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

**INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION**

Volume 3, No. 3, 2013. Odesa – 98 p.

---

**Засновник:** Одеський національний політехнічний університет

Зареєстровано Міністерством юстиції України 04.04.2011р.

Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Одеського національного політехнічного університету (протокол №1 від 30.08.2013)

**Адреса редакції:** Одеський національний політехнічний університет,  
проспект Шевченка, 1, Одеса, 65044 Україна

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

E-mail: [immm.ukraine@gmail.com](mailto:immm.ukraine@gmail.com)

Автори опублікованих матеріалів несуть повну відповідальність за підбір, точність наведених фактів, цитат, економіко-статистичних даних, власних імен та інших відомостей. Редколегія залишає за собою право скорочувати та редагувати подані матеріали

© Одеський національний політехнічний університет, 2013