

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ
МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL
METHODS IN SIMULATION

Том 4, № 2

Volume 4, No. 2

Одеса – 2014
Odesa – 2014

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:

Г.В. Ахмамет'єва

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 - 6460Р of 04.04.2011

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

Associate editor:

A.A. Kobozeva

Executive editor:

H.V. Akhmamet'ieva

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: +38 048 705 8506

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

E-mail: immm.ukraine@gmail.com

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

Tel.: +38 048 705 8506

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

E-mail: immm.ukraine@gmail.com

© Одеський національний політехнічний університет, 2014

ЗМІСТ / CONTENTS

ЗАГАЛЬНИЙ ПІДХІД ДО АНАЛІЗУ
СТАНУ ІНФОРМАЦІЙНИХ СИСТЕМ
ЯК ТЕОРЕТИЧНИЙ БАЗИС ДЛЯ
СТЕГАНОВАЛГОРИТМІВ, СТІЙКИХ
ДО АТАКИ СТИСКОМ

А.А. Кобозєва, М.О. Мельник,
П.Є. Баранов

99

GENERAL APPROACH TO
INFORMATION SYSTEM STATE
ANALYSIS AS THEORETICAL BASIS
FOR STEGO ALGORITHMS ROBUST
AGAINST COMPRESSION ATTACKS

Kobozeva A., Melnik M., Baranov P.

ТЕХНОЛОГІЯ ПРОГРАМУВАННЯ
ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ НА
КЛАСТЕРАХ

В.Д. Павленко

105

TECHNOLOGY PROGRAMMING OF
PARALLEL COMPUTING FOR
CLUSTERS

Pavlenko V.

ВЕЙВЛЕТ-НЕЙРОННИЙ АНАЛІЗ ДЛЯ
ВИЯВЛЕННЯ ДЕФЕКТІВ
АСИНХРОННОГО ДВИГУНА

Б. Боровік, В. Карпінський

111

WAVELET-NEURAL ANALYSIS FOR
INDUCTION MOTOR FAULTS
DETECTION

Borowik B., Karpinskyi V.

РОЗРОБКА МЕТОДИКИ КОНТРОЛЮ
ЯКОСТІ ДРУКОВАНИХ ПЛАТ НА
ОСНОВІ АВТОМАТИЧНОГО
СКРИПТА

Ю.Ю. Козіна

120

DEVELOPING THE METHODOLOGY
FOR PRINTED CIRCUIT CARD
QUALITY CONTROL BASED ON
AUTOMATIC SCRIPT

Kozina Yu.

МОДЕЛЮВАННЯ І ОПТИМІЗАЦІЯ
ПРОЦЕСУ ЗАПОВНЕННЯ РЕСУРСУ
СКЛАДНИХ ОБ'ЄКТІВ

РАДІОЕЛЕКТРОННОЇ ТЕХНІКИ

К.Ф. Боряк, С.В. Ленков, В.М. Цицарєв

126

MODELING AND OPTIMIZATION OF
THE OPERATIONAL LIFE EXTENSION
PROCESS FOR COMPLEX
RADIOELECTRONIC SYSTEMS

Boryak K., Lenkov S., Cicarev V.

ІНФОРМАЦІЙНА МОДЕЛЬ БЕЗПЕКИ
ТЕХНОЛОГІЙ ЗВ'ЯЗКУ

В.Б. Дудікевич, В.О. Хорошко,

Г.В. Микитин, Р.І. Банах, А.І. Ребець

137

INFORMATION SECURITY MODEL
FOR COMMUNICATION
TECHNOLOGIES

Dudikevich V., Khoroshko V.,
Mikitin G., Banach R., Rebets A.

ЗАСТОСУВАННЯ МЕТОДІВ
МАШИННОГО НАВЧАННЯ ДЛЯ
ФОРМУВАННЯ СЦЕНАРІЇВ
ПОВЕДІНКИ ЗЛОВМИСНИХ
ПРОГРАМНИХ ЗАСОБІВ
О.В. Молдавська, В.М. Рувінська

149 USING MACHINE LEARNING
METHODS TO FORM THE SCENARIOS
OF BEHAVIOR OF
MALICIOUS SOFTWARE
Moldavskaya A., Ruvinskaya V.

ГРАФОВА МОДЕЛЬ СТАНІВ
КОРИСТУВАЧА СИСТЕМИ
ДИСТАНЦІЙНОГО НАВЧАННЯ
С.В. Ленков, О.О. Гайша, Є.С. Ленков

158 GRAPH MODEL FOR THE STATES OF
DISTANCE LEARNING SYSTEM USER
Lenkov S., Gaisha A, Lenkov E.

ВИКОРИСТАННЯ СИМВОЛІВ ЯКОБІ
ДЛЯ ГЕНЕРУВАННЯ ПАРАМЕТРІВ
ЕЛІПТИЧНОЇ КРИВОЇ В
КРИПТОСИСТЕМАХ
І.З. Якименко, Л.М. Тимошенко,
В.А. Мокріцький

165 USE OF JACOBI SYMBOLS TO
GENERATE THE ELLIPTIC CURVE
PARAMETERS IN CRYPTOSYSTEMS
Yakimenko I., Timoshenko L.,
Mokritskyi V.

МЕТОД РОЗПІЗНАВАННЯ
ВИХІДНОГО СИГНАЛУ
МУЛЬТИСЕНСОРА ЗА ДОПОМОГОЮ
МОДУЛЬНИХ НЕЙРОННИХ МЕРЕЖ
І.В. Турченко

173 A METHOD TO IDENTIFY A
MULTISENSOR OUTPUT SIGNAL BY
MEANS OF MODULAR NEURAL
NETWORKS
Turchenko I.

МАТЕМАТИЧНІ МОДЕЛІ ТА
УЗАГАЛЬНЕННЯ МАТЕМАТИЧНОГО
ОПISУ ПРОЦЕСІВ ПЕРВИННОЇ
ПЕРЕРОБКИ СИРИХ ВУГЛЕВОДНІВ
Ю. В. Григоренко

180 MATHEMATICAL MODELS AND
GENERALIZATION OF
MATHEMATICAL DEFINITION FOR
PRIMARY PROCESSING OF CRUDE
HYDROCARBONS
Grigorenko Yu.

ОБЩИЙ ПОДХОД К АНАЛИЗУ СОСТОЯНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ КАК ТЕОРЕТИЧЕСКИЙ БАЗИС ДЛЯ СТЕГАНОАЛГОРИТМОВ, УСТОЙЧИВЫХ К АТАКЕ СЖАТИЕМ

А.А. Кобозева, М.А. Мельник, П.Е. Баранов

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

В работе выявлены и обоснованы недостатки при обеспечении устойчивости стеганоалгоритмов к атаке сжатием в случае организации стеганопреобразования в частотной, пространственной/временной области контейнера, в качестве которого выступают цифровые изображения, аудио и видео последовательности. Показано, что одной из основных причин отсутствия окончательного решения обсуждаемой задачи является отсутствие единого теоретического базиса, общего математического подхода к ее решению. Обосновано, что перспективным, с точки зрения построения на его основе стеганоалгоритмов, устойчивых к сжатию, в том числе со значительными коэффициентами, является общий подход к анализу состояния и технологии функционирования информационных систем, основанный на теории возмущений и матричном анализе.

Ключевые слова: стеганоалгоритм, атака против встроенного сообщения, устойчивость к сжатию, общий подход к анализу состояния и технологии функционирования информационных систем

Введение

Стеганографическая система сегодня является одной из наиболее значимых составных частей комплексной системы защиты информации [1]. Компьютерный характер современной стеганографии обусловил широкое использование в качестве контейнеров (в том числе, и в настоящей работе) цифровых изображений, видео, аудио.

При разработке стеганографической системы необходимо учитывать требование устойчивости этой системы к активным атакующим действиям. Одними из наиболее пагубных атак являются атаки против встроенного сообщения [2], имеющие своей целью разрушение конфиденциальной информации, передающейся посредством организации скрытого канала внутри канала общего пользования. К атакам против встроенного сообщения относятся: наложение шума на стеганосообщение (СС), его фильтрация, сжатие с потерями. Последняя из перечисленных атак является сегодня чрезвычайно распространенной благодаря популярности и необходимости использования форматов с потерями для хранения и передачи цифровых сигналов (в частности, цифровых изображений (ЦИ)). По этой же причине действия атакующего, связанные с пересохранением СС в формат с потерями, не привлекают к себе внимание адресатов и могут остаться незамеченными. Организаторы скрытого канала заинтересованы в том, чтобы результат таких действий не привел к разрушению передаваемой информации. Кроме того, учитывая реалии сегодняшнего дня, необходимо отметить, что пересылка ЦИ, аудио, цифрового видео в формате без потерь сама по себе привлекает внимание и вызывает подозрение. Поэтому при организации

стеганографического канала связи для передающей стороны целесообразно использовать форматы с потерями еще на этапе формирования СС.

Из всего вышесказанного очевидным является вывод: при организации скрытого (стеганографического) канала связи необходимо использовать стеганоалгоритмы, устойчивые к сжатию, что даст возможность еще до пересылки сохранять СС в привычном сегодня формате с потерями, не привлекающем внимания (например, Jpeg для ЦИ), а также извлекать дополнительную информацию (ДИ) в случае, если СС подверглось соответствующей атаке.

На сегодняшний день существует значительное количество различных стеганографических алгоритмов (СА), которые позиционируются авторами как устойчивые к сжатию [3-5], однако все эти алгоритмы не лишены значительных недостатков: многие из них не обеспечивают устойчивость к сжатию со значительными коэффициентами, многие не обеспечивают надежность восприятия формируемого СС. Необходимо отметить, что при рассмотрении данной проблемы в современной научной литературе большое внимание уделяется устойчивости к сжатию СА, реализующих погружение цифровых водяных знаков (где надежность восприятия СС часто не требуется), а вот алгоритмы организации скрытого канала связи рассматриваются гораздо реже. Причина этому ясна: сложность одновременного обеспечения устойчивости к сжатию (со значительными коэффициентами) и надежности восприятия СС, обусловленная отсутствием единого теоретического базиса, общего математического подхода для решения рассматриваемых задач. Развитие стеганографии в направлении создания устойчивых к сжатию стеганометодов сегодня идет по экстенсивному пути, при помощи накопления все большего количества различных СА, которые не отличаются друг от друга принципиально, а лишь незначительно улучшают параметры своей работы относительно «предшественников».

Таким образом, *цель* настоящей работы, заключающаяся в выборе математических основ для построения теоретического базиса для разработки стеганографических методов и алгоритмов, гарантированно устойчивых к сжатию, в том числе, со значительными коэффициентами, обеспечивающих надежность восприятия СС, для повышения эффективности работы стеганосистемы, и, как следствие, комплексной системы защиты информации, является *актуальной*.

Основная часть

Анализ современных научных публикаций, касающихся разработки стеганометодов и алгоритмов, устойчивых к атаке сжатием, в том числе, со значительными коэффициентами, приводит к следующим выводам.

Подавляющее большинство СА, позиционируемых как устойчивые к сжатию, производит стеганопреобразование в частотной области контейнера, или основного сообщения (ОС) [4,5], основываясь на спорном в свете [1,6] утверждении, что более устойчивыми к разнообразным искажениям, в том числе, к сжатию, являются СА, использующие для стеганопреобразования именно частотную область. Такие алгоритмы, основываются на компромиссе между требованиями надежности восприятия формируемого СС и устойчивости к сжатию, достигаемом в большинстве случаев за счет использования в процессе стеганопреобразования, главным образом, среднечастотных коэффициентов. Однако этот компромисс не позволяет достичь эффективного декодирования ДИ при значительном сжатии СС, он является определенным ограничителем на повышение эффективности стеганосистемы. Оставаясь в рамках такого подхода, невозможно повышение устойчивости к сжатию разрабатываемых стеганометодов, СА и соответствующих стеганосистем.

В связи с этим интерес вызывают попытки ученых выйти за границы среднечастотной области при организации внедрения ДИ. Но хотя эти попытки и

предпринимаются, они не содержат ничего принципиально нового в подходе к решению рассматриваемой задачи [7-9]. Основными недостатками существующих СА, использующих значимые частотные коэффициенты в процессе организации стеганопреобразования, являются:

- негарантированность обеспечения надежности восприятия СС за счет значительного возмущения матрицы ЦИ при возмущениях низкочастотных коэффициентов;
- для соблюдения надежности восприятия СС при организации стеганопреобразования за счет возмущения низкочастотных коэффициентов ОС эти возмущения необходимо настолько малы, что для декодирования ДИ требуется наличие контейнера, что на практике часто не имеет места.

Подлежит сомнению не только мнение о преимуществе частотной области стеганопреобразования в свете устойчивости стеганосистемы к сжатию. Авторы [10] утверждают, что СА может быть устойчивым к сжатию только тогда, когда он будет учитывать особенности реализации алгоритма перспективного сжатия: алгоритм, устойчивый к сжатию, основанному на вейвлет-преобразовании (Jpeg2000), может оказаться неустойчивым к сжатию, основанному на дискретном косинусном преобразовании (Jpeg). С учетом того, что сжатие является лишь одним из возмущающих воздействий на СС [1], специфика которого – это обнуление высокочастотных составляющих сигнала, такое мнение в общем случае является ошибочным, оно ограничивает возможности для построения СА, устойчивых к компрессии.

Таким образом, в рамках частотной области, используемой для организации стеганопреобразования, обеспечение одновременной устойчивости СА к сжатию со значительными коэффициентами, надежности восприятия СС, организации процесса декодирования без наличия контейнера вызывает непреодолимые трудности. Использование частотной области принципиально не позволяет проводить дальнейшее увеличение устойчивости разрабатываемых стеганоалгоритмов к сжатию.

Организация стеганопреобразования в рамках пространственной/временной области контейнера [3] в общем случае также не может гарантировать устойчивости СА: все пиксели матрицы ЦИ, кадра видеопоследовательности, отсчеты цифрового аудио равноправны; изменения каких-либо из них (например, максимальных, минимальных, стоящих на определенных местах и т.д.) не отвечают, в общем случае, каким-либо определенным частотным характеристикам. Крайне затруднительно в пространственной/временной области управлять процессом, связанным с необходимостью изменений конкретных частотных составляющих сигнала.

Таким образом, для интенсификации процесса решения рассматриваемой задачи требуется выход за пределы частотной, пространственной/временной областей контейнера для организации стеганопреобразования, использование новых математических инструментов и подходов.

Перспективным с точки зрения построения на его основе стеганоалгоритмов, устойчивых к сжатию, в том числе, со значительными коэффициентами, является общий подход к анализу состояния и технологии функционирования информационных систем (ОПАИС), основанный на теории возмущений и матричном анализе [1].

Основная идея этого подхода заключается в следующем. ЦИ, видео, а также аудио последовательность формально можно представить в виде одной или конечного множества двумерных матриц. В силу этого в качестве ОС, не ограничивая общности рассуждений, для простоты изложения рассматривается ЦИ в градациях серого с матрицей F . Результат стеганопреобразования, независимо от способа и области погружения ДИ, формально представляется в виде совокупности возмущений полного набора параметров [1], определяющих матрицу ОС (или матрицы блоков ОС). При этом последующие изменения СС, в том числе и в результате активных атакующих действий

(в частности, атаки сжатием), формализуются в виде дополнительных возмущений полного набора параметров. В качестве такого набора может использоваться набор сингулярных чисел (СНЧ) и ортонормированных лексикографически положительных сингулярных векторов (СНВ) соответствующих матриц, однозначно определяемых их нормальным сингулярным разложением, целесообразность использования которого подробно обоснована в [1] (везде ниже, если не оговорено особо, сингулярные векторы рассматриваются в ортонормированном лексикографически положительном виде). Таким образом, результат сжатия СС с потерями формально представляется как совокупность возмущений СНЧ и СНВ соответствующей матрицы (матриц) СС.

В [1,6] показано, что свойства СА, в том числе, их устойчивость к активным атакующим действиям, определяются величинами и локализацией возмущений СНЧ и СНВ матриц, отвечающих контейнеру, произошедших в ходе стеганопреобразования, а не областью, используемой для стеганопреобразования.

Все вышесказанное и результаты, изложенные в [1,6], приводит к следующим значимым для рассматриваемой задачи выводам, говорящим о преимуществах ОПАИС перед используемыми до настоящего момента подходами как основы для разработки устойчивых стеганоалгоритмов:

1. СНЧ и СНВ принципиально отличаются по своим свойствам от совокупности частотных коэффициентов, которые также однозначно определяют матрицу ЦИ и использование которых традиционного при организации стеганопреобразования, в частности, коэффициентов дискретного косинусного преобразования. Если

$$F = U_F \Sigma_F V_F^T$$

— нормальное сингулярное разложение матрицы F [1], где U_F, V_F — ортогональные матрицы левых и правых СНВ F соответственно, столбцы U_F — лексикографически положительны, а $\Sigma_F = \text{diag}(\sigma_1(F), \dots, \sigma_n(F))$ — матрица СНЧ, то каждая сингулярная тройка

$$(\sigma_i(F), u_i(F), v_i(F)),$$

где $u_i(F), v_i(F)$ — левый и правый СНВ, соответствующие $\sigma_i(F)$, несет в себе в той или иной мере информацию обо всех частотных составляющих сигнала-изображения (при этом максимальные СНЧ — главным образом, о низкочастотных составляющих, а минимальные — о высокочастотных) [1,6]. А это значит, что возмущение даже одного СНЧ/СНВ в процессе стеганопреобразования в той или иной мере «растворит» погруженную информацию во всех частотных составляющих контейнера; возмущение максимальных СНЧ при погружении ДИ затронет не только низкочастотные коэффициенты дискретного косинусного преобразования матрицы ЦИ-контейнера (хотя именно они возмущаются в этом случае больше всего, по сравнению с другими [1,6], что и будет обеспечивать нечувствительность СС к сжатию со значительными коэффициентами [1]), но и все остальные, что уменьшит «удар» на низкие частоты, повышая при этом вероятность обеспечения надежности восприятия СС. Такой принципиально новый подход опосредованного «размазывания» дополнительной информации по всем частотным составляющим при организации стеганопреобразования должен позволить получить более устойчивые к сжатию СА, обеспечивающие надежность восприятия соответствующего СС, по сравнению с теми СА, которые основывались на возмущениях исключительно в частотной области ОС.

2. С учетом того, что анализ свойств СА в свете ОПАИС часто сводится к анализу возмущений СНЧ матрицы (блоков матрицы) ЦИ [1], важно отметить, что

такой анализ является более предпочтительным в вычислительном смысле по сравнению с анализом возмущений яркости пикселей в пространственной области или частотных коэффициентов изображения, что имеет большое значение, особенно при работе с видео последовательностями. Действительно, для $n \times n$ -матрицы изображения количество пикселей, как и частотных коэффициентов равно n^2 , в то время как сингулярных чисел на порядок меньше - n .

Таким образом, использование общего подхода к анализу состояния и технологии функционирования информационных систем является на сегодняшний день наиболее перспективным для разработки на его основе стеганоалгоритмов, устойчивость которых к сжатию превысит этот параметр для существующих аналогов.

Выводы

В работе обосновано, что при организации скрытого канала связи внутри канала общего пользования на современном этапе развития инфокоммуникационных технологий целесообразно использовать стеганоалгоритмы, необходимо устойчивые к атаке сжатием.

В работе выявлены и обоснованы недостатки при обеспечении устойчивости стеганоалгоритмов к сжатию с потерями в случае организации стеганопреобразования в частотной, пространственной/временной области контейнера, в качестве которого выступают цифровые изображения, аудио или видео последовательности.

Показано, что одной из основных причин отсутствия окончательного решения обсуждаемой задачи является отсутствие единого теоретического базиса, общего математического подхода к ее решению.

Обосновано, что перспективным с точки зрения построения на его основе стеганоалгоритмов, устойчивых к сжатию, в том числе, со значительными коэффициентами, является общий подход к анализу состояния и технологии функционирования информационных систем, основанный на теории возмущений и матричном анализе, принципиально позволяющий организовать процесс стеганопреобразования таким образом, чтобы, наряду с устойчивостью, повысить вероятность обеспечения надежности восприятия стеганосообщения по сравнению с существующими аналогами.

Список литературы

1. Кобозева, А.А. Анализ защищенности информационных 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.
2. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
3. Lancini, R. A robust video watermarking technique in the spatial domain / R. Lancini, F. Mapelli, S. Tubaro // Proceedings of Video/Image Processing and Multimedia Communications 4th EURASIP-IEEE Region 8 International Symposium on VIPromCom, Zadar, Croatia, 16–19 June 2002. — 2002. — PP. 251–256.
4. Shih, F.Y. Combinational image watermarking in the spatial and frequency domains / F.Y. Shih, S.Y.T. Wu // Pattern Recognition. — 2003. — Vol. 36, Iss. 4. — PP. 969–975.
5. Suhail, M.A. Digital watermarking based DCT and JPEG model / M.A. Suhail, M.S. Obaidat // IEEE Transactions on Instrumentation and Measurement. — 2003. — Vol. 52, Iss. 5. — PP. 1640–1647.
6. Кобозева, А.А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации // Искусственный интеллект. — 2007. — № 4. — С. 531–538.

7. Fridrich, J. Combining Low-Frequency and Spread Spectrum Watermarking / J. Fridrich // Proceedings of the SPIE Conference on Mathematics of Data/Image Coding, Compression and Encryption, July 19, 1998, San-Diego, USA. — 1998. — Vol.3456. — PP. 2–12.
8. Huang, J. Image digital watermarking algorithm using multiresolution wavelet transform // J. Huang, C. Yang // Proceeding of the IEEE International Conference on Systems, Man and Cybernetics, 10–13 Oct. 2004. — 2004. — Vol. 3. — PP. 2977–2982.
9. 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.
10. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.

ЗАГАЛЬНИЙ ПІДХІД ДО АНАЛІЗУ СТАНУ ІНФОРМАЦІЙНИХ СИСТЕМ ЯК ТЕОРЕТИЧНИЙ БАЗИС ДЛЯ СТЕГАОАЛГОРИТМІВ, СТІЙКИХ ДО АТАКИ СТИСКОМ

А.А. Кобозєва, М.О. Мельник, П.С. Баранов

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

У роботі виявлені й обґрунтовані недоліки при забезпеченні стійкості стеганоалгоритмів до атаки стиском у випадку організації стеганоперетворення в частотній, просторовій/часовій області контейнера, у якості якого виступають цифрові зображення, аудіо й відео послідовності. Показано, що однією з основних причин відсутності остаточного рішення обговорюваної задачі є відсутність єдиного теоретичного базису, загального математичного підходу до її рішення. Обґрунтовано, що перспективним з погляду побудови на його основі стеганоалгоритмів, стійких до стиску, у тому числі, зі значними коефіцієнтами, є загальний підхід до аналізу стану й технології функціонування інформаційних систем, заснований на теорії збурень і матричному аналізі.

Ключові слова: стеганоалгоритм, атака проти вбудованого повідомлення, стійкість до стиску, загальний підхід до аналізу стану й технології функціонування інформаційних систем.

GENERAL APPROACH TO INFORMATION SYSTEM STATE ANALYSIS AS THEORETICAL BASIS FOR STEGO ALGORITHMS ROBUST AGAINST COMPRESSION ATTACKS

A.A. Kobozeva, M.A. Melnik, P.E. Baranov

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

Shortcomings in the process of provision of stegoalgorithms with robustness to compression attacks were identified and proved for the case of stegotransformation in frequency, spatial/time domain of a cover object, with digital images, audio and video series used as cover objects. It was shown that lack of a comprehensive theoretical basis and general mathematical approach to the solution process for the problem discussed is one of the basic reasons for absence of the final solution. It was justified that general approach to information system state and functioning analysis based on perturbation theory and matrix analysis is a promising one for the development of robust to compression attacks stegoalgorithms, including those with significant coefficients.

Keywords: stegoalgorithm, attack against the embedded message, robustness against compression, general approach to information system state and functioning analysis

ТЕХНОЛОГИЯ ПРОГРАММИРОВАНИЯ ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛЕНИЙ НА КЛАСТЕРАХ

В.Д. Павленко

Одесский национальный политехнический университет,
пр. Шевченко, 1, Одесса, 65044, Украина; e-mail: pavlenko_vitalij@mail.ru

Рассматриваются принципы организации кластерных вычислений с помощью неявного распараллеливания, основанного на понятии заказа, а также особенности новой, альтернативной MPI, технологии распараллеливания вычислений, позволяющей для достаточно широкого класса вычислительных алгоритмов естественным образом переходить от существующих последовательных реализаций к параллельным.

Ключевые слова: параллельные вычисления, кластеры, технология программирования параллельных вычислений, архитектура программного обеспечения

Введение

Параллельные вычисления достаточно динамично развиваются в последнее время [1-4], что обусловлено, в первую очередь, появлением все более сложных задач, решение которых на современных последовательных ЭВМ за приемлемое время получить невозможно. К ним относятся задачи идентификации и моделирования нелинейных динамических систем на основе моделей Вольтерра [5-7], задачи информационной оптимизации, возникающие при проектировании систем модельной диагностики [8, 9], цифровой фильтрации изображений [10] и др. В данное время интерес к параллельным вычислениям также во многом связан со все большим распространением многоядерных процессоров [11].

Для эффективного создания параллельных приложений следует учитывать особенности применяющейся параллельной архитектуры [2]. Здесь в качестве такой архитектуры выбраны кластеры. Кластер представляет собой набор компьютеров, процессоры которых не имеют общей памяти, а обмениваются данными через сеть [12]. Главным преимуществом кластеров является их низкая стоимость, поскольку во многих случаях используются обычные массовые ПК и традиционные сетевые технологии; кластер может быть просто временно организован из простаивающих компьютеров какой-либо сети. Главным недостатком кластеров является скорость передачи данных между отдельными процессорами, которая является относительно низкой из-за отсутствия общей памяти. Это приводит либо к необходимости использования альтернативных сетевых технологий, либо к сужению класса эффективно реализуемых алгоритмов.

Одной из задач, полностью пока не решенных, является задача создания инструментальных средств параллельного программирования. Одним из основных препятствий для создания подобных инструментальных средств является сложность обнаружения участков кода в программе, которые могут выполняться параллельно. В случае же, если в используемой параллельной архитектуре процессоры не имеют общей памяти, реализация обмена данными обычно тоже является одной из задач прикладного программиста.

Существуют два основных подхода для снятия этого препятствия. Первый состоит во внесении в язык программирования средств декларирования потенциального параллелизма, примерами его применения являются технология OpenMP, языки программирования NORMA и Haskell. Второй – в предоставлении пользователю мощных низкоуровневых средств организации взаимодействия процессоров, примерами его применения являются технология MPI и инструментарий Globus Toolkit. В данное время преимущественно используется второй подход, поскольку он позволяет добиться более высокой эффективности параллельных приложений за счет предоставления прикладному программисту более мощных средств контроля над используемой параллельной вычислительной системой. Обратной стороной данного подхода является более высокая сложность разработки и отладки параллельных приложений и перенос акцента в процессе разработки приложения с реализации алгоритма прикладной задачи к реализации работы со средствами, предлагаемыми выбранной технологией параллельного программирования.

Первый подход предпочтителен в задачах со сложным взаимодействием процессоров в ходе выполнения, возможностью внесения существенных изменений в логику распараллеливания в процессе развития программ. Преимущества первого подхода являются еще более заметными в случае отсутствия априорных сведений о составе кластера, поскольку наличие в программе именно сведений о потенциальном параллелизме, а не конкретных операций взаимодействия процессоров, позволяет реализовать достаточно сложные средства балансировки нагрузки.

Принципы технологии транспарентного распараллеливания на основе заказов

Предположим, что в распараллеливаемой программе выделен набор процедур, в процессе работы которых не модифицируются никакие переменные, кроме параметров и временно создаваемых структур данных, а входные и выходные параметры передаются по значению. Выполнение программы при этом должно сводиться к выполнению одной из этих процедур. Подобное предположение налагает достаточно существенные ограничения на программу. Например, оно запрещает всякую работу с глобальными переменными и устройствами ввода-вывода. Однако, как будет показано далее, подобное предположение относительно программы может быть ослаблено. Так, процедурам можно дать возможность работы с глобальными переменными или устройствами ввода-вывода при соблюдении некоторых условий.

Для иллюстрации предлагаемой технологии рассмотрим участок программы, схематическое изображение которого представлено на рис. 1, где прямоугольником обозначается время выполнения процедуры, отсчитываемое слева направо. Для обозначения вложенных процедур используются вложенные прямоугольники. Длины прямоугольников и их частей пропорциональны времени, затрачиваемому на выполнение соответствующих фрагментов программы. Линиями изображаются связи, которые объединяют моменты вычисления некоторых данных с моментами, когда они впервые используются в дальнейших вычислениях, при этом изображая только связи для данных, вычисляемых во вложенных процедурах, и используемых в основной процедуре или другой вложенной процедуре.

Первый принцип, на котором основан предлагаемый метод распараллеливания, заключается в понятии заказа на вычисления. Заказ на вычисления вводится как единица выполняемой на одном из компьютеров кластера работы, т.е. объем работы, который обязан быть выполнен на одном из компьютеров кластера полностью и не может быть разбит на более мелкие части. В качестве такого объема работы вводится выполнение одной процедуры без выполнения тех процедур, которые она вызывает: выполнение каждой из них выделяется в отдельный заказ. Для того чтобы определить

точку старта программы, одна из процедур должна быть описана как главная. Именно через параметры этой процедуры должны передаваться исходные данные и результаты вычислений.

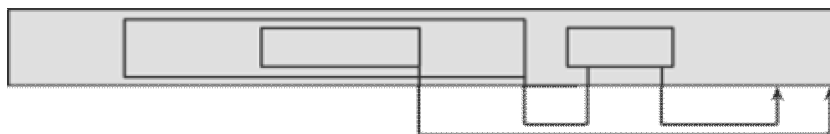


Рис.1. Схематическое изображение участка программы для распараллеливания

Этот принцип иллюстрирует рис. 2 (считается, что возникающие за время работы четыре заказа будут выполняться на четырех различных процессорах, а их выполнение будет начинаться сразу же). Для наглядности показаны связи по данным между частями процедур. Прерывистыми линиями выделены части вычислительного процесса, производимые на одном процессоре.

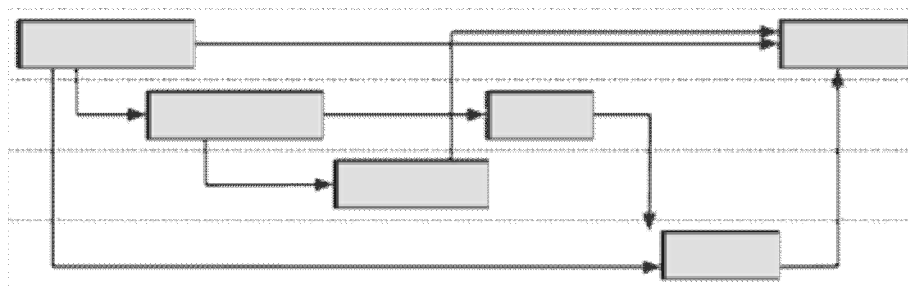


Рис. 2. Иллюстрация первого принципа технологии распараллеливания

В значительном числе алгоритмов существует отрезок времени между получением некоторых данных и первым их использованием в дальнейших вычислениях; часто он может быть увеличен путем внесения изменений в порядок вычислений, не изменяющих результат. Наличие таких промежутков, связано с возможностью распараллеливания алгоритма, поскольку при их отсутствии работа данного алгоритма не может быть распараллелена никакими средствами. Вторым принципом является следующее. При традиционном подходе при вызовах процедур вызывающая процедура продолжает свою работу только после окончания работы вызываемой процедуры – или, иными словами, вызывающая процедура начинает ожидание результатов выполнения вызываемой процедуры в момент вызова, а заканчивает в момент завершения вызываемой процедуры. Вместо этого предлагается начинать ожидание в момент, когда данные, вычисляемые вызываемой процедурой, требуются для дальнейших вычислений (если в этот момент они уже вычислены, то начинать ожидание не нужно), и заканчивать ожидание в момент, когда эти данные получены. Этот принцип иллюстрирует рис. 3.

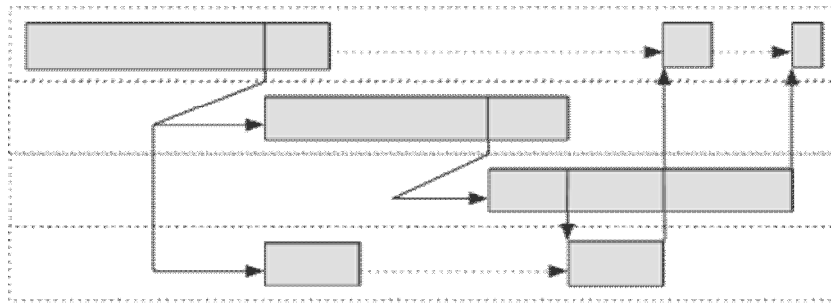


Рис. 3. Иллюстрация второго принципа технологии распараллеливания

Легко видеть, что такой график выполнения может быть получен из предыдущего максимально возможным сдвигом влево всех вычислений, при котором соблюдается следующее условие: всякое значение используется уже после того, как оно вычислено.

Архитектура программного обеспечения

Предлагаемая технология реализована в виде инструментальных программных средств на языке программирования Java [13]. Архитектура программного обеспечения приведена на рис. 4.

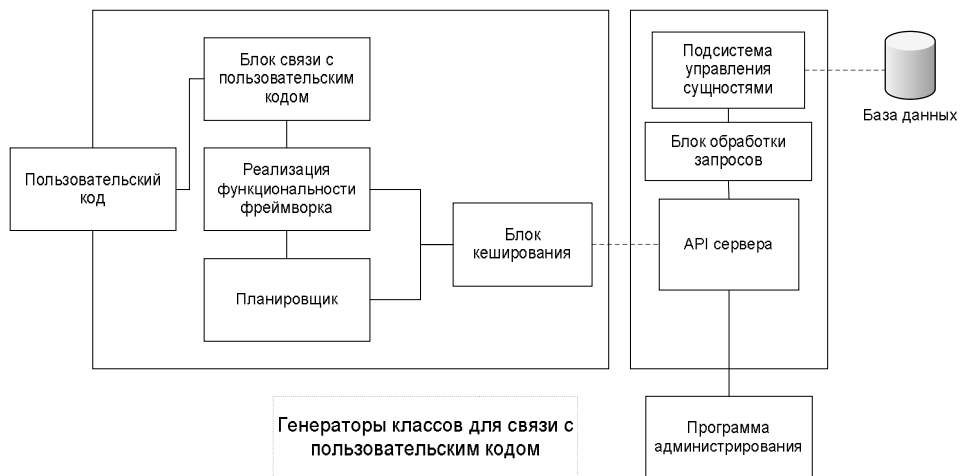


Рис. 4. Архитектура программного обеспечения

Серверная часть должна обеспечивать выполнение по запросам от клиентов следующих функций: отправки заказа, получения заказа, отправки значения, получения значения и отправки уведомления о завершении выполнения заказа. Также для отладки параллельных приложений к набору этих функций добавлены функции для получения текущего времени на сервере и вывода отладочного сообщения в создаваемый на сервере файл. Базовыми понятиями, возникающими в процессе взаимодействия клиента и сервера, являются заказ, идентификатор значения и идентификатор неизвестного значения.

Задача клиентской части – получение заказов с сервера и их выполнение, но также в состав этой части включены средства для отправки пользовательских заказов. Клиентская часть должна предоставлять пользовательскому коду функции отправки

заказа и получения значения величины; именно эти функции реализует часть клиента, ответственная за взаимодействие с пользовательским кодом. Следует пояснить наличие блока кэширования в клиентской части, введение которого связано с необходимостью снижения нагрузки на сеть. Этот блок хранит в себе полученные от сервера значения для некоторых идентификаторов значений и часть информации о связях между идентификаторами значений и идентификаторами неизвестных значений, а также о связях между идентификаторами неизвестных значений. Это позволяет не производить повторное получение данных, если они уже были недавно получены.

Функциональность, доступная пользователю, заключена в нескольких классах. Во-первых, это генерируемый класс библиотеки, который для каждой из выделенных пользователем процедур содержит метод для отправки заказа на выполнение этой процедуры. Список выделенных процедур при этом должен декларироваться пользователем в .XML файле, причем для каждой процедуры должно быть задано ее расположение, имя генерируемого метода, а также для каждого параметра – тип, имя и направление. Во-вторых, это класс `ServConnector`, содержащий средства для работы с расположенными на сервере файлами и добавления записей в лог-файл, ведущийся на сервере. В-третьих, это класс `DataHandler`, от которого должны быть порождены все классы, использующиеся в качестве типов параметров процедур. Пользователю доступны две группы методов этого класса:

- Абстрактные методы для сериализации и восстановления состояния. Для передачи параметров процедур не используется стандартный механизм сериализации, поскольку при передаче выходных параметров их значения нужно вносить в уже существующие объекты, в то время как стандартный механизм позволяет лишь создать новый объект. Поэтому реализуемые пользователем классы должны реализовывать эти методы.

- Методы `preRead()`, `preChange()`, `preReplace()`, которые должны вызываться перед обращением к данным, частичным изменением данных и полной заменой содержимого объекта соответственно. Для потомков этого класса вводится правило, что они должны предоставлять доступ к содержащимся в них данным только через свои методы, в которых вызываются эти три унаследованных метода, где это необходимо. Методы `preRead` и `preChange` убеждаются, что в объекте есть данные, а `preReplace` сбрасывает флаг о том, что в объекте нет данных, если он был установлен. Введение двух методов `preRead` и `preChange` позволяет, если после сериализации данных объекта производился только доступ на чтение, обнаруживать эту ситуацию и не производить второй раз сериализацию.

Выводы

Предлагаемый подход, в отличие от технологии MPI, предполагает, что программа, реализованная с его использованием, является набором инструкций, управляющим работой кластера в целом, а не его отдельного компьютера. Из этого следует применимость предложенного подхода: это алгоритмы, естественно реализуемые с использованием параллелизма заданий. Учитывая сложности с использованием технологии MPI в применении к параллелизму заданий, предложенная технология в этой области может рассматриваться как альтернатива традиционно используемой технологии MPI.

Список литературы

1. Антонов, А.С. Параллельное программирование с использованием технологии MPI / А.С. Антонов– М.: Изд-во МГУ, 2004. – 71 с.

2. Воеводин, В.В. Параллельные вычисления / В. В. Воеводин, Вл. В. Воеводин. – СПб.: БХВ-Петербург, 2002. – 608 с.
3. Gebali, F. Algorithms and Parallel Computing / F. Gebali – Publisher: Wiley, 2012. – 364 p. - ISBN-10: 0470902108 -ISBN-13: 978-0470902103
4. Buyya, R. Cloud Computing Principles and Paradigms / R. Buyya, J. Broberg, A. M. Goscinski. Publisher: Wiley, 2011. – 664 p. - ISBN:0470887990
5. Kolding, T. E. High-order Volterra Series Analysis Using Parallel Computing / T. E. Kolding, T. Larsen // International Journal of Circuit Theory and Applications. – 1997. - 25, 2. - 107-114 p. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.46.7254&rep=rep1&type=pdf>
6. Pavlenko, V.D. Interpolation Method of Nonlinear Dynamical Systems Identification Based on Volterra Model in Frequency Domain / V.D. Pavlenko, S.V. Pavlenko, V.O. Speranskyy // Proceedings of the 7th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2013), 15–17 September 2013, Berlin, Germany – P. 173–178.
7. Pavlenko, V. Identification of systems using Volterra model in time and frequency domain / V.D. Pavlenko, S.V. Pavlenko, V.O. Speranskyy // In book: «Advanced Data Acquisition and Intelligent Data Processing» / V. Haasz and K. Madani (Eds.) – River Publishers, 2014 - P. 233-270.
8. Korbicz, J. Modeling, Diagnostics and Process Control: Implementation in the DiaSter System/ J. Korbicz, J. M. Kościelny – Berlin: Springer, 2010. – 384 p.
9. Pavlenko, V. Technology for Data Acquisition in Diagnosis Processes By Means of the Identification Using Models Volterra / V. Pavlenko, O. Fomin, V. Ilyin // Proc. of the 5th IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2009), Rende (Cosenza), Italy, September 21–23, 2009. – P. 327-332.
10. Тхань, Ф.Н. Параллельная реализация алгоритмов фильтрации космических изображений / Фьонг Нгуен Тхань, А.Ю. Шелестов // Проблемы управления и информатики. – 2005. – № 5. – С. 121 – 132.
11. Шпаковский, Г.И. Реализация параллельных вычислений: кластеры, многоядерные процессоры, грид, квантовые компьютеры. – Минск : БГУ, 2010. – 155 с.
12. Основные классы современных параллельных компьютеров / Internet-ресурс: <http://parallel.ru/computers/classes.html>
13. Burdejnyj, V.V. Method of practical usage of orders based transparent parallelizing technology / V.V. Burdejnyj, V. D. Pavlenko // Труды Одесск. политехн. ун-та. – Одесса, 2012. – Вып. 1 (37). – С. 227-233.

ТЕХНОЛОГІЯ ПРОГРАМУВАННЯ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ НА КЛАСТЕРАХ

В.Д. Павленко

Одеський національний політехнічний університет,
пр. Шевченко, 1, Одеса, 65044, Україна; e-mail: pavlenko_vitalij@mail.ru

Розглядаються принципи організації кластерних обчислень за допомогою неявного розпаралелювання, заснованого на понятті замовлення, а також особливості нової, альтернативної MPI, технології розпаралелювання обчислень, що дозволяє для досить широкого класу обчислювальних алгоритмів природним чином переходити від існуючих послідовних реалізацій до паралельних.

Ключові слова: паралельні обчислення, кластери, технологія програмування паралельних обчислень, архітектура програмного забезпечення

TECHNOLOGY PROGRAMMING OF PARALLEL COMPUTING FOR CLUSTERS

V.D. Pavlenko

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

Principles of organization of the cluster computing using implicit parallelism based on the notion of order, and also features a new, alternative MPI, parallel computing technology, allowing for a fairly wide class of computational algorithms in a natural way to move from existing serial to parallel implementations.

Keywords: parallel computing, clusters, technology programming parallel computing, software architecture

WAVELET-NEURAL ANALYSIS FOR INDUCTION MOTOR FAULTS DETECTION

B. Borowik¹, V. Karpinskyi²

¹ University of Bielsko-Biala,
ul. Willowa 2, 43-309 Bielsko-Biala, Poland,

² The TechnoCentre of Coventry University,
Priory Street, Coventry, United Kingdom, CV1 5FB, e-mail: mpkarpinski@gmail.com

This paper presents a method of fault identification of induction motor drive by means of the application of wavelet analysis of a tested signal and a model of neural network with supervised learning, and also a model of neural network processed in the next epochs by means of algorithm making essential changes of parameters of this network. The tests which were executed on three important state variables, describing physical quantities of the chosen induction motor drive model confirmed the usefulness of the method used for diagnostic purposes, allowing the identification of the fault type occurring in the induction motor drive in the initial phase of formation.

Keywords: induction motor drive, wavelet transformation, network learning rule.

Introduction

Diagnostics of electromechanical processes is involved in the recognition of undesirable changes of their states, which will be presented in the form of a series of intentional actions executed in a fixed time by the determined set of machines and devices with specified and available resources. Faults and other destructive events can be caused by changes of these states. The diagnostic system should as soon as possible detect and identify occurring faults already in their initial formation phase. The destructive events resulting from an increasing time of exploitation and use are recognized as some kind of faults, which must be detected and identified after exceeding some value.

Currently, methods of modeling of the faults and their identification, designed on the basis of artificial intelligence techniques, are being applied intensively in diagnostics of industrial processes.

The signals of electromechanical systems contain some information which is the basis of diagnostic analysis. Therefore, attention should be focused on extraction and use of the information contained in those signals. As a result of analysis of these signals in different fields, e.g. simultaneously in the fields of time and frequency, simpler interpretation of meanings and different features of these signals is possible. Thus, there is also a simpler interpretation of attributes assigned to different undesirable states of the system.

Classification of signals simultaneously in the field of time and frequency is possible by use of transformation methods allowing research of his spectral properties. Tested signal is presented as a linear combination of some basic orthogonal signals. This method minimizes the signal model. In order to minimize the set of relevant decomposition's coefficients shapes of the basis function must be adapted to the analysed signal.

The wavelet analysis is one of the popular and more often used methods of spectral analysis. This analysis contrary to the Fourier analysis does not express analysed functions by polynomials built on harmonic functions but by special functions – waves, which are made with the function of the so-called mother wave designed for this purpose. Created wavelet

functions are put to multiple translations. Obtained in this way set of basic functions of the transformation has many important, scalable properties, which can be related to the time as well as the frequency, analyzing relationships between the tested function and its transformed coefficients.

As a result of localization of wavelets in time and frequency domains, the wavelet signal processing in comparison to sinusoids is suitable for those signals whose spectral content changes over time. The adaptive time-frequency resolution of wavelet signal processing allows us to perform multiresolution analysis.

Methodology and simulations of diagnostic algorithm of fault's identification

Simulations were executed for nominal conditions of asynchronous induction motor drive, whose model was built in the stationary system of coordinates referring to stator (model $\alpha, \beta, 0$). The induction motor drive was burdened by the working machine, with the character of the dynamic mass-absorbing-resilient element. Figure 1 shows the connection of the working machine with the induction motor drive.

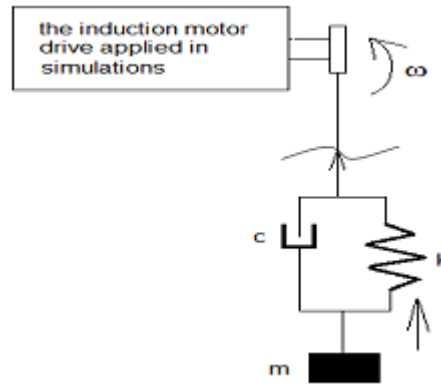


Fig. 1. Diagram of the dynamic mass-absorbing-resilient element which was connected to the induction motor drive applied in simulations.

The simulation model of the induction motor drive was realised in the environment MATLAB/Simulink. The following parameters of induction motor drive were fixed in executed simulations (applied induction motor drive is the substitute diagram and the following parameters are expressed in the relative units): $r_s = 0.059$, $r_w = 0.048$, $x_s = 1.92$, $x_w = 1.92$, $x_m = 1.82$, $w = x_s x_w - x_m^2 = 0.374$, $T_m = 0.86$ [s].

Simulations were executed on two neural networks for wavelet decomposition's coefficients of three state ariables describing physical quantities: stator's current i_s , angle speed ω and linear acceleration A . The results of simulations for every physical quantity were written in matrix M .

For all tests (in four groups of simulations) there were fixed the same values: (the coefficient of springiness) $k = 100$ [N/m], radius $r = 0.15$ [m], $m = 10$ [kg]. In the next groups of simulations value of the viscous friction's coefficient c was fixed: $c = 0.8$ [Ns/m], $c = 1.0$ [Ns/m], $c = 1.25$ [Ns/m] and $c = 1.5$ [Ns/m].

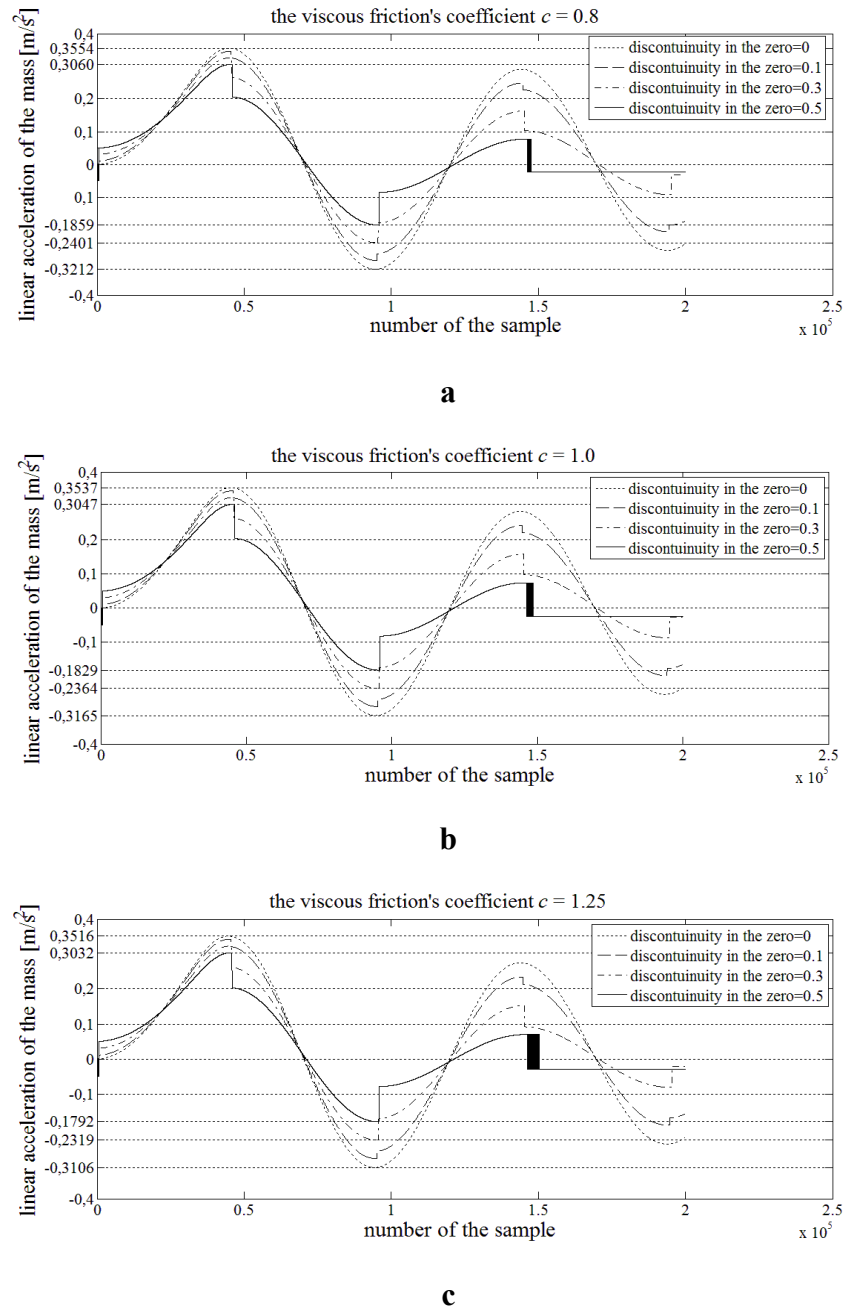


Fig. 2. Waveforms of characteristics of linear acceleration of the dynamic mass-absorbing-resilient element's mass: a – viscous friction's coefficient $c = 0.8$; b – viscous friction's coefficient $c = 1.0$; c – viscous friction's coefficient $c = 1.25$

Results of simulation of fault's identification

On the basis of exemplary results with complex done simulations of state variables, it is possible to notice that the obtained results of correct minimal value in the matrix Mse_2 are bigger in comparison to the results obtained in matrix Mae_1 and Mse_1 for the correct fault's identification. Besides this it is necessary to state on the basis bad exemplary results that minimal values of matrix Mse_1 repeats in results for the same simulation. In such cases identification of fault's number is possible only by means of minimal value of matrix Mse_2 . In executed simulations the fixed value of the second neural network's learning coefficient

$l_k = 0.3$ caused bad identification of occurring fault's number. Most of the good results of identification of fault's number were obtained for the following parameters:

- value of the stopping condition of the first neural network's learning $\delta = 0.5$;
- value of the first neural network's learning coefficient $l = 0.9$;
- increasing of number epochs of the second neural network's processing from 3 to 12;
- increasing of the second neural network's learning coefficient l_k from 0.3 to 0.95.

It is necessary to state on the basis of exemplary good results of minimal values of matrices Mse_1 and Mse_2 that the next increase of the number of epochs in the second neural network from value 6 as well as the next increase of the learning coefficient l_k from value 0.6 does not cause the change of the final result of identification of fault's numbers for wavelet decomposition's tested coefficients of the chosen state variables describing physical quantities in the experiment. From the results it has been possible to notice that a small value of learning coefficient l_k and big value δ does not assure the correct fault's identification even with an increase of the number of epochs in the second neural network.

As a result of the decreasing value δ and the increase of the number of epochs in the second neural network, it has been possible to notice a more profitable effect of improvement of the identification of fault's number. The process of identification of the fault begins in a moment when the expression determined in the left part of following inequality is bigger than insensibility's zone determined in the right part of this inequality:

$$\sum_{j=1}^{750} \varepsilon_1 |M_{1(j)} - M_{(1,j)}| > \sum_{j=1}^{750} \varepsilon_2 |M_{2(j)} - M_{(1,j)}|, \quad (1)$$

where:

$M_{1(j)}$ – matrix registered for the unknown fault of stator's resistance from wavelet decomposition's tested coefficients of state variables describing three physical quantities in experiment: stator's current i_s , angle speed ω and linear acceleration A ;

$M_{(1,j)}$ – matrix registered from wavelet decomposition's tested coefficients of state variables describing three physical quantities in experiment: stator's current i_s , angle speed ω and linear acceleration A (1 – the number of the index in matrix M and concerns good induction motor drive);

$M_{(j)}$ – matrix registered for stator's resistance r_s of good induction motor decreased about 0.25% her nominal value into the bottom from wavelet decomposition's coefficients of three state variables describing physical quantities in the experiment: stator's current i_s , angle speed ω and linear acceleration A ;

ε_1 – coefficient fixed in simulations, in the case coefficients of stator's current i_s and linear acceleration A is fixed $\varepsilon_1 = 1$, however in case angle speed's coefficients ω is fixed $\varepsilon_1 = 100$;

j – number of the index of chosen sample with matrix M .

Otherwise the process of identification of the fault will be finished.

The idea of diagnostic algorithm consists of indication of the occurrence of fault's number. This number is determined by means of calculating the smallest values of matrices: Mse_1 and Mse_2 . The values of matrices Mse_1 and Mse_2 were calculated by means of parameters obtained as a result of training of neural network with supervising learning, and also a model of neural network processed in next epochs by means of algorithm making

essential changes of parameters of this network. This neural network has one layer of neurons. The diagram of this neural network is presented on figure 3.

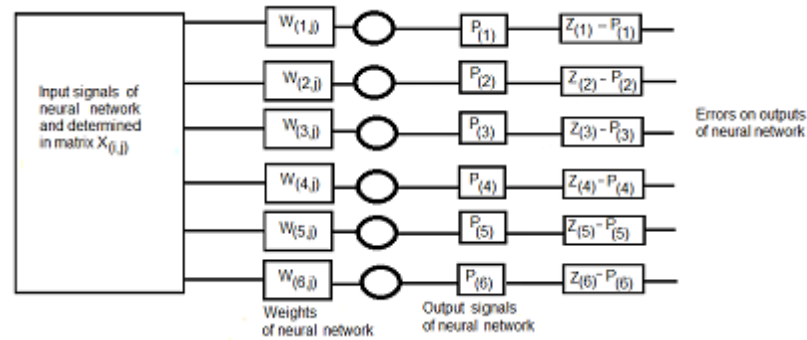


Fig. 3. Diagram of the applied neural network with supervised learning according to the rule delta. The presented circles represent neurons in neural network.

It was fixed that input signals of neural network X were calculated according to the formula:

$$X_{(i,j)} = \forall_{i=1,2,\dots,6} \sum_{j=1}^{750} \varepsilon_1 |M_{1(j)} - M_{(1,j)}|, \quad (2)$$

where:

$M_{1(j)}$ – matrix is described by the formula (1),

$M_{(1,j)}$ – matrix is described by the formula (1),

ε_1 – coefficient is described by the formula (1),

i – a number of neural network's neuron.

The aim of this training is to find values of neural network output signals P , for which values of weights W are the best for obtainment of the appropriate smallest value of matrix Mse_2 necessary for the correct identification of fault's number.

Advantage of this neural network is a linear layer in which each neuron has such same the set of input signals X as well as such same initial values of matrix of weights W .

Additionally, adoption of such a set of input signals X for each neuron causes faster finishing of this neural network's learning. The initial values of matrix's $W_{(i,j)}$ were calculated according to the formula:

$$W_{(i,j)} = \forall_{\substack{i=1,2,\dots,6 \\ j=1,2,\dots,750}} (M_{(1,j)} - mean)^2, \quad (3)$$

where:

$M_{(1,j)}$ – matrix is described by the formula (1),

$mean$ – the arithmetic mean of matrix $M_{(1,j)}$,

i – number of neuron and is described by the formula.

The arithmetic mean of matrix $M_{(1,j)}$ was calculated according to the formula:

$$mean = \frac{\sum_{j=1}^{750} M_{(1,j)}}{750}. \quad (4)$$

In the purpose of proper assurance of learning's process, weights W must be selected, so that output signals P like the most correspond to determined target values Z on neural network's outputs in moment of finishing of neural network's learning.

Output signals of neural network P were calculated according to the formula:

$$P_{(i)} = \forall_{i=1,2,...,6} \sum_{j=1}^{750} W_{(i,j)} X_{(i,j)}, \quad (5)$$

where:

$X_{(i,j)}$ – matrix is described by the formula (2),

$W_{(i,j)}$ – matrix of neural network's weights and is described by the formula (3).

The learning pattern of this network contains two components: input data X and target values Z for these input data and is always presented in next epochs of neural network's learning.

Appropriate determination of the neural network's target signals Z decide about faster finishing of this neural network's learning with the obtainment of the best results for identification of fault's number.

The target values on neural network's outputs Z were calculated according to the formula:

$$Z_{(i)} = \forall_{\substack{i,l=1,2,...,6 \\ k=1,2,...,7}} \varepsilon_2 \sum_{j=1}^{750} |M_{(l+1,j)} - M_{(k,j)}|, \quad (6)$$

where:

$M_{(l,j)}, M_{(k,j)}$ – matrices registered for all possible cases of faults stator's resistance decreased about 1% to 20 % into the bottom of its nominal value for wave-let decomposition's tested coefficients of state variables describing three physical quantities in experiment: stator's current i_s , angle speed ω and linear acceleration A ,

ε_2 – coefficient fixed in simulations, in the of case the coefficients stator's current i_s and linear acceleration A is fixed, $\varepsilon_2 = 1$, however in case angle speed's coefficients ω is fixed $\varepsilon_2 = 10$,

i – number of neurons and is described by the formula (2),

k, l – numbers of the index of matrix M .

Index $k=1$ in matrix $M_{(k,j)}$ represents case for good induction motor drive. Determination of the neural network's target values Z and input signals X as well as correction of weights W is necessary for calculation of errors on neurons E . This calculation follows always after presentation the learning pattern in next epochs of the learning process of this neural network. Values of errors on neurons E were calculated according to the formula

$$E_{(i)} = \forall_{i=1,2,...,6} (Z_{(i)} - P_{(i)}), \quad (7)$$

where:

$P_{(i)}$ – matrix is described by the formula (5),

$Z_{(i)}$ – matrix is described by the formula (6).

In learning process of neural network is possible to find iteratively appropriate for purposes of fault's identification values of matrix W . Updating of weights of this neural network is possible after each presentation of one learning pattern and according to the adopted rule of changing their. According to this rule, after presentation of the learning pattern correction of weight will follow as a result of earlier weight correction about the product of difference between target value on output Z , and obtained value on neuron's output P and also input's value X , from which this weight is associated. Additionally in the adopted rule values of input signals X are decreased as a result of multiplication of their with experimentally selected neural network's learning coefficient l . Correction of weights in the next epochs of neural network's learning was calculated on the basis of the well-known rule delta according to the formula:

$$W_{(i,j)} = \forall_{\substack{i=1,2,\dots,6 \\ j=1,2,\dots,750}} W_{(i,j)} + l X_{(i,j)} E_{(i)}, \quad (8)$$

where:

$E_{(i,j)}$ – matrix is described by the formula (7),

$W_{(i,j)}$ – matrix is described by the formula (3),

$X_{(i,j)}$ – matrix is described by the formula (2),

l – learning coefficient of neural network is fixed in range from 0 to 1.

A commonly used cost is the *Root-Mean Squared* error RMS , which after presentation of the learning pattern in next epochs of neural network's learning tries to minimize the error E between the output values P and the target values Z over all the exemplary pairs X and W in the purpose of the obtainment of the smallest value of matrix Mse_2 .

Advantage of this neural network is speed of obtainment of stopping condition of the neural network learning despite of necessity and difficulties resulting with adoption of values of input signals X and target values Z .

The *Root-Mean Squared* error RMS was calculated according to the formula

$$RMS = \sqrt{\frac{\sum_{i=1}^6 (E_{(i)})^2}{6}}, \quad (9)$$

where $E_{(i,j)}$ is a matrix described by the formula (7).

It was fixed that neural network was learnt in a moment of condition's obtainment

$$RMS < \delta, \quad (10)$$

where δ is a value fixed experimentally in executed simulations for the necessity of stopping of applied neural network's.

Conclusions

Simulations presented in this work confirmed that the occurrence of small step changes of stator's resistance r_s decreased in percentage terms into the bottom her nominal value at sampling frequency 50 kHz gives in the determined conditions a noticeable effect in the form of changes of wavelet decomposition's tested coefficients of state variables describing

physical quantities: linear acceleration on circuit of motive wheel of rotor A , stator's current i_s and also angle speed of rotor ω .

This effect is more noticeable in the case of correct selection of the wave kind and its order referring to transitory course's shape of the tested physical quantity.

The results of executed simulations confirmed that for a model induction motor drive, which usually is described by nonlinear characteristics of elements, information contained in wavelet decomposition's coefficients can be used in the process of reasoning the kind and localization of fault's occurring of this model's elements.

References

1. Theory of Digital Automata. Series: Intelligent Systems, Control and Automation: Science and Engineering, Vol. 63 / B. Borowik, M. Karpinsky, V. Lahno, O. Petrov. – Dordrecht Heidelberg New York London: Springer. – 2013. – 206 p. – ISBN 978-94-007-5227-6.
2. Borowik, B. Interfacing PIC Microcontrollers to Peripheral Devices / B. Borowik // Science and Engineering. – New York: Springer Verlag. – 2011. – 178 p. – ISBN 94-007-1118-2.
3. Douglas, H. Detection of broken rotor bars induction motors using wavelet analysis / H. Douglas, P. Pillay, A. Ziarani // International IEEE Conference On Electric Machines and Drive. IEMDC. – 2003. – Vol. 2. – P. 923-928.
4. Mehala, N. Rotor Faults Detection in Induction Motor by Wavelet Analysis / N. Mehala, R. Dahiya // International Journal of Engineering Science and Technology. – 2009. – Vol.1(3). – P. 90-99.

ВЕЙВЛЕТ-НЕЙРОННИЙ АНАЛІЗ ДЛЯ ВИЯВЛЕННЯ ДЕФЕКТІВ АСИНХРОННОГО ДВИГУНА

Б. Боровік¹, В. Карпінський²

¹ University of Bielsko-Biala,
ul. Willowa 2, 43-309 Bielsko-Biala, Poland,

² The TechnoCentre of Coventry University,

Priory Street, Coventry, United Kingdom, CV1 5FB, e-mail: mpkarpinski@gmail.com

У статті представлено метод ідентифікації дефектів приводу з асинхронним двигуном, використовуючи вейвлет-аналіз досліджуваних сигналів і модель нейронної мережі. Наведено модель нейронної мережі, перетворюваної на чергових наступних етапах на підставі алгоритму, за допомогою якого вносяться істотні зміни параметрів цієї мережі. На основі проведених досліджень для трьох важливих змінних стану, які описують фізичні величини обраної моделі асинхронного електроприводу, підтверджено придатність запропонованого методу для проведення діагностики, що дає змогу ідентифікувати характер пошкоджень в даному приводі на початковій стадії виникнення.

Симуляцію моделі асинхронного двигуна здійснено в середовищі Matlab Simulink. В подальшому виконано моделювання на основі нейронних мереж, підтримуючи вейвлет-розкладання для трьох змінних стану. За допомогою цих змінних стану описано такі фізичні величини: струм ротора, кутову швидкість, лінійне прискорення. Всі результати, отримані на базі обчислень за допомогою нейронної мережі, надалі збережено у відповідній матриці.

Для реалізації алгоритму діагностики застосовано нейронну мережу, що має один шар нейронів. Нейронні мережі навчено згідно з прийнятим алгоритмом для знаходження найменшого значення матриці. Доведено, що отримане найменше значення матриці є корисним для правильної діагностики випробуваного двигуна. Результатами проведеної симуляції підтверджено, що модельований асинхронний двигун можна діагностувати щодо джерел дефектів в двигуні на підставі вейвлет-розкладання та інформації, зібраної під час аналізу із застосуванням нейронних мереж.

Ключові слова: асинхронний двигун, вейвлет-перетворення, правило мережевого навчання.

ВЕЙВЛЕТ-НЕЙРОННИЙ АНАЛІЗ ДЛЯ ВИЯВЛЕННЯ ДЕФЕКТОВ АСИНХРОННОГО ДВИГАТЕЛЯБ. Боровик¹, В. Карпинский²¹ University of Bielsko-Biala,
ul. Willowa 2, 43-309 Bielsko-Biala, Poland,² The TechnoCentre of Coventry University,
Priory Street, Coventry, United Kingdom, CV1 5FB, e-mail: mpkarpinski@gmail.com

В статье представлен метод идентификации дефектов привода с асинхронным двигателем, используя вейвлет-анализ для исследуемых сигналов и модель нейронной сети. Приведена модель нейронной сети, преобразованной на очередных последующих этапах на основании алгоритма, при помощи которого вносятся существенные изменения параметров этой сети. На основе проведенных исследований для трех важных переменных состояния, которые описывают физические величины выбранной модели асинхронного электропривода, подтверждена пригодность предложенного метода для проведения диагностики, что дает возможность идентифицировать характер повреждений в данном приводе на начальной стадии возникновения.

Симуляция модели асинхронного двигателя осуществлена в среде Matlab Simulink. В дальнейшем выполнено моделирование на основе нейронных сетей, поддерживая вейвлет-разложение для трех переменных состояния. С помощью этих переменных состояния описаны такие физические величины: ток ротора, угловую скорость, линейное ускорение. Все результаты, полученные на базе вычислений с помощью нейронной сети, в дальнейшем сохранены в соответствующей матрице.

Для реализации алгоритма диагностики применена нейронная сеть, которая имеет один слой нейронов. Нейронные сети обучены согласно принятому алгоритму для нахождения наименьшего значения матрицы. Доказано, что полученное наименьшее значение матрицы является полезным для правильной диагностики испытуемого двигателя. Результатами проведенной симуляции подтверждено, что моделируемый асинхронный двигатель можно диагностировать относительно источников дефектов в двигателе на основании вейвлет-разложения и информации, собранной во время анализа с применением нейронных сетей.

Ключевые слова: асинхронный двигатель, вейвлет-преобразование, правило сетевого обучения.

РАЗРАБОТКА МЕТОДИКИ КОНТРОЛЯ КАЧЕСТВА ПЕЧАТНЫХ ПЛАТ НА ОСНОВЕ АВТОМАТИЧЕСКОГО СКРИПТА

Ю.Ю. Козина

Одесский национальный политехнический университет,
пр. Шевченко, 1, Одесса, 65044, Украина; e-mail: yuliyakc@mail.ru

Работа посвящена разработке методики контроля качества печатных плат на основе автоматического скрипта. Актуальность исследований подтверждается необходимостью создания систем контроля, которые будут целесообразно использовать в условиях мелкосерийного производства, а также разработки автоматических скриптов в целях сокращения затрат времени для контроля. Предложенная система обладает высокими показателями помехоустойчивости, а методика контроля их качества ускоряет процесс проверки.

Ключевые слова: печатная плата, реперные знаки, программная система, автоматический скрипт.

Введение

В настоящее время требования практики производства изделий микроэлектроники, например, печатных плат, делают актуальной задачу разработки систем контроля их качества, использующих недорогое оборудование. Это связано с возрастающей стоимостью контроля, выполняемого на основе существующих программных комплексов, применение которых обосновано в случае крупносерийного производства и потребностью производства мелких и средних партий изделий. Снижение стоимости таких комплексов возможно за счет уменьшения требований к техническим параметрам аппаратуры, которая используется для контроля [1]. Существующие комплексы контроля включают подсистемы формирования, регистрации и распознавания изображений. Снижение требований к техническим параметрам аппаратуры комплексов приводит к появлению помех при обработке изображений контролируемого изделия. Поэтому предложено разработать программную систему, обладающую высоким уровнем помехоустойчивости и позволяющую выполнять контроль качества печатных плат в условиях помех с высоким уровнем достоверности. В свою очередь, проведение экспериментов на больших объемах данных для подтверждения высокой помехоустойчивости системы и достоверности контроля качества печатных плат ручным способом приводит к росту временных затрат на эту процедуру. Требования практики разработки систем контроля качества изделий микроэлектроники, которые обладают высокой помехоустойчивостью и необходимостью автоматизации процесса их проверки на базе разработанных систем делают актуальной данную работу.

Цель статьи и постановка задачи

Целью работы является разработка методики контроля качества печатных плат на базе предложенной программной системы для сокращения затрат времени на эту процедуру. Одним из методов контроля качества печатных плат, который реализуется в существующих комплексах контроля и позволяет выделять их дефекты, является метод позиционирования эталонного и контролируемого изображений по реперным знакам (специально наносимым на поверхность платы объектов известной формы).

Основная часть

При анализе процессов, которые реализуются в существующих комплексах контроля показано, что основными процедурами, определяющими достоверность контроля в условиях помех, являются локализация и классификация реперных знаков. Существующие методы локализации и классификации изображений не обеспечивают достаточную достоверность контроля в условиях помех [2]. При разработке соответствующих методов локализации и классификации к обрабатываемому изображению было применено гиперболическое вейвлет-преобразование (ГВП) [3, 4]. Преимущество применения ГВП, по сравнению с градиентными методами, заключается в том, что оно:

- предоставляет возможность выбора масштаба вейвлет-преобразования (длины носителя) s , что позволяет выделять объекты нужных размеров и обеспечивает необходимую для решения задачи контроля качества печатных плат точность и помехоустойчивость;
- повышает помехоустойчивость с увеличением масштаба вейвлета;
- концентрирует энергию изображения в области перепадов интенсивности, что повышает точность при поиске объекта.

Так, например, применение ГВП при локализации объектов позволяет путем увеличения масштаба преобразования s (длины носителя гиперболического вейвлет-фильтра) расширить пространственную локализацию объектов. При этом изменяются значения амплитуды сигнала в пространстве ГВП, которые соответствуют перепадам интенсивности исходного изображения. Объектам меньшей протяженности соответствуют меньшие значения ГВП. Кроме того, за счет свойств ГВП обладает высокими показателями помехоустойчивости – существующие методы обработки изображений, основанные на данном виде преобразования работоспособны при отношениях сигнал/шум не менее 5 (по мощности).

ГВП определено как непрерывное вейвлет-преобразование с функцией [5]:

$$\Omega_0(\tau) = \frac{1}{\pi\alpha\tau} G(\tau), \quad (1)$$

где τ – независимая переменная;

$G(-\tau) = G(\tau)$ – адаптирующая функция, $G(\tau) = 1(\tau - \varepsilon) - 1(\tau - \gamma)$;

$1(\tau)$ – единичная функция Хевисайда;

$\alpha > 0$ – масштабный множитель для получения базисных вейвлетных функций;

ε, γ – параметры адаптирующей функции.

Здесь $0 < \varepsilon \ll \gamma$, поэтому такой выбор $\Omega_0(\tau)$ избавит материнский вейвлет от сингулярности функции $\frac{1}{\pi\tau}$ в точке $\tau = 0$, сохранив ее свойства при сколь угодно малом $\varepsilon > 0$, а выбор γ обеспечит достаточную локализацию. Доказано, что при

использовании в качестве базисной, функция $\Omega_0(\tau)$ (материнский вейвлет) удовлетворяет всем свойствам, предъявляемым при построении вейвлет-преобразования [6]. В [7] предложено выполнить замену функции $G(\tau)$, на функцию $G_1(\tau)$. На основе этого при построении базисной функции для обеспечения высокой помехоустойчивости и точности в соответствии со спецификой решаемой задачи, в работе выбрана такая адаптирующая функция [4]:

$$G_1(\tau) = \begin{cases} \frac{1}{\alpha\tau}, & |\tau| > \varepsilon; \\ \frac{\tau}{\varepsilon}, & |\tau| \leq \varepsilon. \end{cases} \quad (2)$$

где τ – независимая переменная. Эмпирически определены ($\alpha = 0.8$; $\varepsilon = 0.1$)

В данной работе предложена программная система контроля качества печатных плат, которая за счет применения разработанных методов локализации и классификации на базе ГВП для разработки соответствующих процедур, позволила получать информацию о выделенных дефектах. Рассмотрим два этапа работы этой системы: режим обучения и рабочий режим. В режиме обучения на входе формируется исходное полутоновое изображение эталона. Для формирования обучающей выборки проводится локализация, поиск, выделение и прослеживание контуров реперных знаков. Производится идентификация на основе информации о характерных точках (ХТ) и рассчитанных геометрических моментов-признаков (ГМП). Информация сохраняется в базу знаний (БЗ). Выполняется обучение многослойного персептрона на основе сформированной обучающей выборки с помощью метода на основе ГВП.

В рабочем режиме на вход системы подается изображение контролируемой печатной платы, полученное с помощью видеокамеры (рис. 1). Производится предварительная обработка входного изображения. Реализуются процедуры локализации и идентификации реперных знаков. Выполняется их распознавание на основе обученной нейронной сети. Реализуется позиционирование изображений эталонной и контролируемой печатной платы. На выходе получаем результат выделения дефектов и их характеристики (координаты местоположения на изображении печатной платы) (рис. 2).

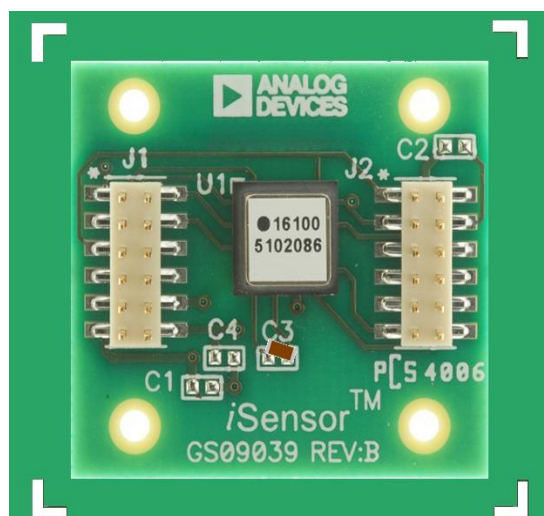


Рис. 1. Изображение контролируемой печатной платы

В целях оценки работоспособности системы и получения оценок ее помехоустойчивости, использована база данных, состоящая из 100 изображений печатных плат, отличающихся размером, углом наклона, уровнями освещенности. В связи со значительным ростом временных затрат на загрузку изображений, а также выполнение всех процедур их обработки, было принято решение разработать автоматический скрипт.

Разработка автоматических скриптов – это новая совокупность знаний и навыков, которые необходимы для того, чтобы, используя инструментальные средства, создавать тестовые процедуры после того, как они были спроектированы и спланированы [8].

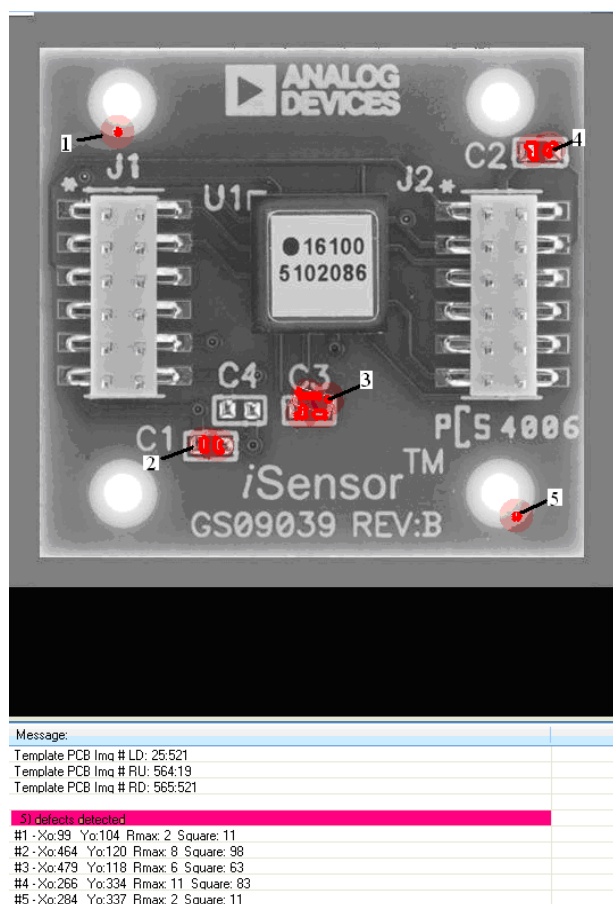


Рис. 2. Результат выделения дефектов и их характеристики

Одним из наиболее популярных, востребованных и весомых программных комплексов для автоматизации тестирования приложений на данный момент является программный комплекс QuickTest Professional (QTP). В данной работе предложена методика контроля качества печатных плат на основе разработки автоматического скрипта. Для его создания используется технология Data Table, которая позволяет параметризовать данные, а также средство проверки результатов прохождения теста.

Методика контроля качества печатных плат на основе автоматического скрипта включает следующие шаги:

1. Указать в настройках QTP путь к приложению.
2. Создать новый тест и добавить соответствующую акцию для его реализации.
3. Создать хранилище объектов – Object Repository для данной программной системы.
4. Выполнить обучение системы для распознавания объектов и их свойств.

5. Провести ассоциацию созданной акции с добавленным хранилищем объектов.

6. Добавить точки проверки: check points – в те части теста, в которых есть необходимость проверки соответствия фактических результатов прохождения теста ожидаемым.

7. Запустить тест для одной итерации и проанализировать результаты.

8. Параметризовать данные.

В результате реализации скрипта получены такие оценки помехоустойчивости системы контроля качества печатных плат: при отношении сигнал шум достоверность контроля в условиях помех в диапазоне отношения сигнал/шум 8...10 (по мощности) составила 94 %.

Разработанный скрипт использует объект DataTable, который является переработанной Excel таблицей, которая параметризует входные значения для организации итеративного процесса ввода различных наборов входных данных. В качестве параметра выступает исходное обрабатываемое изображение платы, что позволяет автоматически подгружать изображение из имеющейся базы. QTP содержит инструмент просмотра, анализа и обработки результатов тестирования – Run Results Viewer. Он позволяет после запуска теста получить информацию об успешно пройденных или не пройденных итерациях. Исходя из полученных результатов, можно сделать вывод об успешно пройденных итерациях теста (рис. 3).

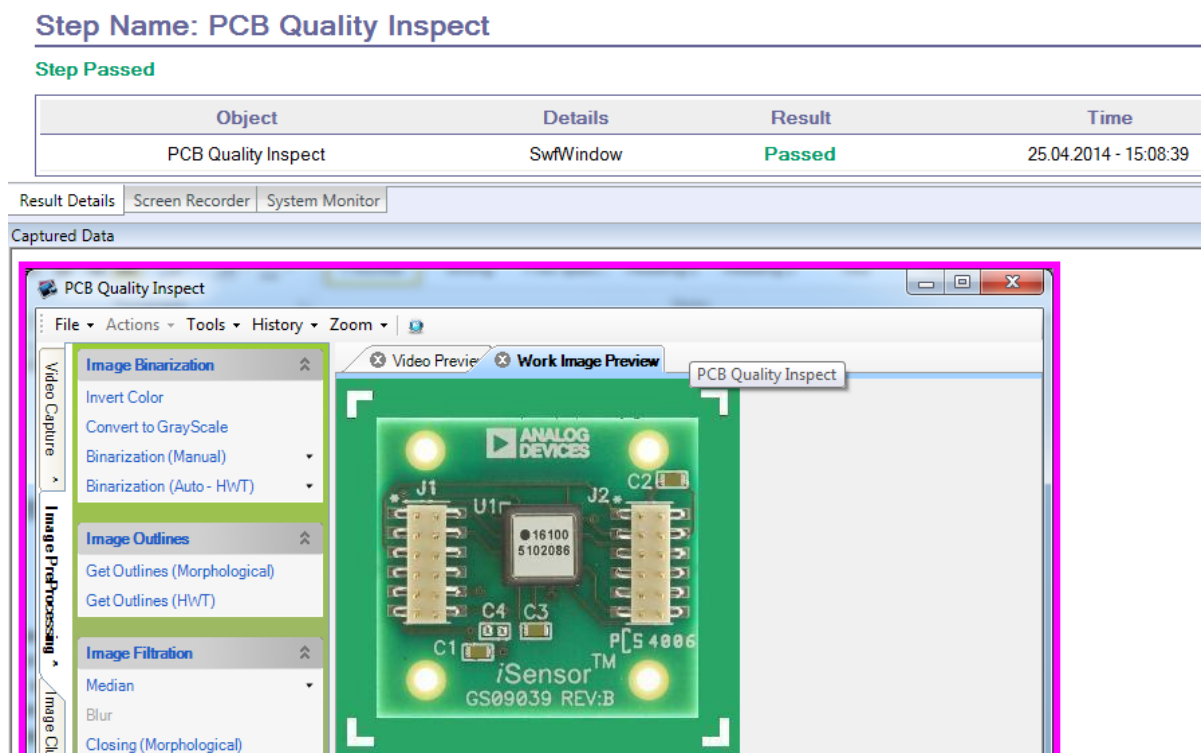


Рис. 3. Результат пройденных итераций теста

Выводы

Эксперименты показали, что в результате применения гиперболического вейвлет-преобразования для реализации процедур локализации и классификации реперных знаков, удалось выделять дефекты на изображениях печатных плат в условиях помех. Методика контроля качества печатных плат, основанная на современных средствах

разработки автоматических скриптов, позволила сократить затраты времени в среднем до 35% по сравнению с ручным методом.

Список литературы

1. Грачев, А.А. Поверхностный монтаж при конструировании и производстве электронной аппаратуры / А. А. Грачев, А.А. Мельник, Л.И. Панов. – ЦНТЭПИ ОНЮА. –2003. – 427 с.
2. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. –М.: Техносфера. – 2005. – 1072 с.
3. Антошук, С.Г. Обработка изображений в области гиперболического вейвлет-преобразования / С.Г. Антошук, В.Н. Крылов // Межвузовский журнал Автоматика. Автоматизация. Электротехнические комплексы и системы. — Херсон, 2003. — №2. — с.7-10.
4. Крылов, В.Н. Позиционирование изображений фотошаблонов в системах автоматизированного оптического контроля / В.Н. Крылов, Г.Ю. Щербакова, Ю.Ю. Козина // Технология и конструирование в электронной аппаратуре. – Одесса, 2007. № 3(69). – С. 61 – 64.
5. Крылов, В.Н. Поиск характерных фрагментов при распознавании объектов с помощью моделей зрительного анализатора/ В.Н. Крылов, С.Г. Антошук // Электроника и связь. – Киев, 2001. –№ 10. – С.73 – 75.
6. Клих, Ю.А. Адаптивные базисные функции вейвлетного преобразования / Ю.А. Клих, С.Г. Антошук, А.А. Николенко // Труды Одес. политехн. ун-та. – Одесса, 2004. – Вып. 2(22). – С.121 — 125.
7. Крылов, В.Н. Контурная сегментация изображений в пространстве гиперболического вейвлет-преобразования с использованием математической морфологии / В.Н. Крылов, М.В. Полякова, Н.П. Волкова // Информационно-измерительные системы. – 2006 . – №2(18) . – С. 35–40.
8. Блэк, Р. Ключевые процессы тестирования. Планирование, подготовка, проведение, совершенствование /Р Блэк. – Москва: Лори. – 2006. — 125 с.

РОЗРОБКА МЕТОДИКИ КОНТРОЛЮ ЯКОСТІ ДРУКОВАНИХ ПЛАТ НА ОСНОВІ АВТОМАТИЧНОГО СКРИПТА

Ю.Ю. Козіна

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

Робота присвячена розробці методики контролю якості друкованих плат на основі автоматичного скрипта. Актуальність досліджень підтверджується необхідністю створення систем контролю, які буде доцільно використовувати в умовах дрібносерійного виробництва виробів, а також розробки автоматичних скриптів в цілях скорочення витрат часу для контролю. Запропонована система має високі показники завадостійкості, а методика контролю їх якості прискорює процес перевірки.

Ключові слова: друкована плата, реперні знаки, програмна система, автоматичний скрипт.

DEVELOPING THE METHODOLOGY FOR PRINTED CIRCUIT CARD QUALITY CONTROL BASED ON AUTOMATIC SCRIPT

Yu. Yu. Kozina

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

The paper is related to the development of the methodology for quality control of printed circuit cards based on automatic script. The development of both quality control systems appropriate for small-batch production and automatic scripts providing for reduction of time required for quality control is a burning issue. The quality control system and methodology proposed offer robust and less time-consuming quality control process, respectively.

Keywords: printed circuit card, reference signs, software system, automatic script.

МОДЕЛИРОВАНИЕ И ОПТИМИЗАЦИЯ ПРОЦЕССА ВОСПОЛНЕНИЯ РЕСУРСА СЛОЖНЫХ ОБЪЕКТОВ РАДИОЭЛЕКТРОННОЙ ТЕХНИКИ

К.Ф.Боряк¹, С.В. Ленков², В. Н. Цыцарев²

¹ Одесская государственная академия технического регулирования и качества,
ул. Ковальская 15, Одесса, 65020, Украина

² Військовий інститут Київського національного університету імені Тараса Шевченка,
вул. Ломоносова, 81, Київ, 03680, Україна, e-mail: lenkov_s@ukr.net

В статье проведено моделирование и оптимизация процесса выполнения ресурса сложных объектов радиоэлектронной техники. Предлагается критерий для определения ресурса восстанавливаемых объектов РЭТ. Вводится понятие процесса выполнения ресурса объектов РЭТ и формулируется задача его оптимизации. Разработан новый алгоритм определения оптимальных параметров этого процесса.

Ключевые слова: радиоэлектронная техника, технический объект, ресурс.

Введение

Ресурс является одной из важнейших надежностных характеристик сложных объектов радиоэлектронной техники (РЭТ), поэтому в процессе эксплуатации объектов РЭТ всегда планируются и осуществляются меры по своевременному восполнению ресурса.

Согласно [1,2] ресурс любого технического объекта (технический ресурс) – это «суммарная наработка объекта с начала его эксплуатации или ее возобновления после ремонта до перехода в предельное состояние». Под предельным состоянием (ПС) понимается «состояние объекта, при котором дальнейшая эксплуатация его недопустима или нецелесообразна, либо восстановление его работоспособности невозможно или нецелесообразно» [1,2].

Эти общие (стандартные) определения в равной степени относятся как к восстанавливаемым, так и к невосстанавливаемым объектам. Для невосстанавливаемых объектов понятие ПС совпадает с понятием отказа и, следовательно, ресурс невосстанавливаемого объекта – это просто наработка до отказа. Для восстанавливаемых объектов (рассматриваемые объекты РЭТ являются восстанавливаемыми) смысл понятия ПС более сложен, так как при определении ПС необходимо учитывать предполагаемые последующие действия после перехода в ПС: прекращать эксплуатацию и списывать (разбирать и утилизировать) объект, производить ремонт для восполнения ресурса, продолжить применение объекта с теми или иными ограничениями. То есть, при определении ресурса для объектов РЭТ необходимо учитывать возможные последующие действия, которые могут предприниматься после наступления ПС. Тем не менее, очевидно, что в основе понятия ресурса все же лежит свойство безотказности объекта, поэтому при определении критерия ПС нужно использовать какой-либо показатель безотказности.

Наиболее информативной характеристикой свойства безотказности восстанавливаемого объекта является параметр потока отказов [1,2]. На протяжении времени «жизни» объекта величина параметра потока отказов изменяется, поэтому его нужно рас-

смагивать как функцию $\Omega(t)$, аргументом которой является суммарная наработка. Традиционно принято считать, что существуют три периода «жизни» радиоэлектронной аппаратуры (РЭА), различающиеся по уровню и характеру поведения показателей безотказности: 1) «период приработки», 2) «период нормальной эксплуатации» и 3) «период износа и старения». На рис. 1 показан типичный вид функции $\Omega(t)$.

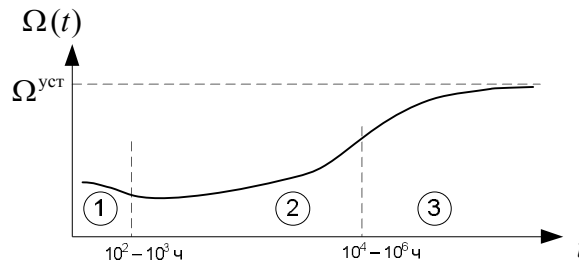


Рис. 1. Вид функции $\Omega(t)$ в течение времени «жизни» объекта РЭТ.

В период приработки возникают так называемые производственные отказы, обусловленные дефектами производства. После замены отказавших элементов, имевших производственные дефекты, уровень безотказности объекта РЭТ повышается (параметр потока отказов уменьшается). Для современной РЭА период приработки практически отсутствует, что достигается благодаря применению при изготовлении объекта новых технологий. В период нормальной эксплуатации вначале уровень безотказности стабилизируется на некоторое время и затем начинает монотонно возрастать. Это возрастание продолжается до тех пор, пока не будет достигнуто установившееся значение $\Omega^{уст}$, соответствующее установившемуся процессу отказов-восстановлений всех элементов объекта. Таким образом, так называемый период износа и старения «растягивается» на десятки (теоретически – на сотни) лет, граница между периодом нормальной эксплуатации и периодом износа и старения оказывается размытой. Для высоконадежных объектов параметр потока отказов вообще не достигает значения $\Omega^{уст}$ за все время «жизни» объекта. Это затрудняет задачу определения ПС объекта и в некоторых случаях делает ее вообще не актуальной. В статье будем полагать, что объект РЭТ в пределах заданного периода эксплуатации является стареющим и для него имеет смысл задавать некоторое предельно допустимое (критическое) значение параметра потока отказов Ω^{nc} . Поэтому примем, что критерием наступления ПС является условие

$$\Omega(t) \geq \Omega^{nc}. \quad (1)$$

С учетом этого величину ресурса объекта R можно определить из уравнения

$$\Omega(R) = \Omega^{nc}. \quad (2)$$

Возможен и другой, менее жесткий подход к определению ресурса, при котором в условии (1) вместо функции $\Omega(t)$ используется ее среднее значение

$$\bar{\Omega}(t) = \frac{1}{t} \int_0^t \Omega(x) dx. \quad (3)$$

С использованием функции $\bar{\Omega}(t)$ критерий (1) приобретает такой вид:

$$\overline{\Omega}(t) \geq \Omega^{nc}. \quad (4)$$

Очевидно, что при одном и том же значении Ω^{nc} ресурс R , получаемый из уравнения $\overline{\Omega}(R) = \Omega^{nc}$, всегда будет больше, чем величина ресурса, полученного из уравнения (2). Поэтому критерий (4) является менее жестким, чем критерий (1).

Предложенные критерии (1) и (4) основываются на знании функции $\Omega(t)$, которая, к сожалению, редко бывает точно известна. В лучшем случае ее вид становится известным к моменту времени, когда эксплуатация объектов данного типа уже завершена, и поэтому ее знание уже может быть не актуальным. Поэтому на практике единственным реальным способом получения функции $\Omega(t)$ остается моделирование. При последующих построениях в данной статье предполагается, что функция $\Omega(t)$ известна и получается методом имитационного статистического моделирования.

Процесс восполнения ресурса объекта радиоэлектронной техники

Для большинства типов объектов РЭТ после наступления ПС их «жизнь» не заканчивается, так как экономически более выгодно восполнить ресурс объекта путем проведения ремонта и затем продолжить его эксплуатацию. Чем больше объем ремонта (чем большая часть элементов заменяется при ремонте), тем большая величина ресурса восполняется при ремонте. Ремонты, предназначенные для восполнения ресурса, как правило, планируются заранее, поэтому будем называть их плановыми ремонтами (ПР).

На рис. 2 показан примерный вид функции $\Omega(t)$ в случае, если проводятся ПР и межремонтный ресурс для ПР определяется по критерию (1).

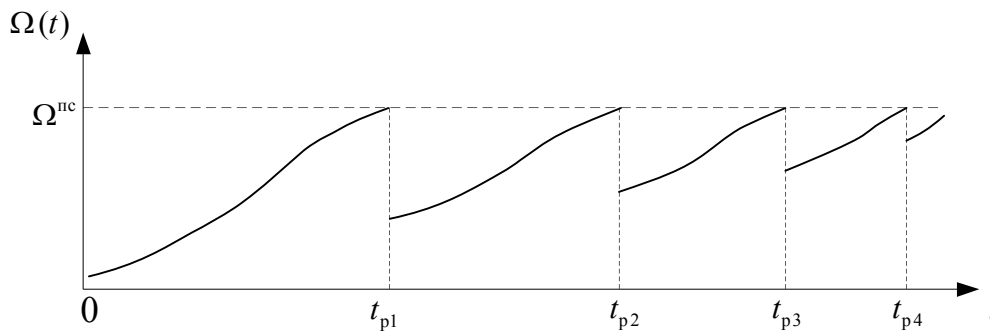


Рис. 2. Вид функции $\Omega(t)$ при проведении ПР по критерию (1).

Процесс восполнения ресурса формально определим как последовательность пар следующего вида:

$$\Psi = \left\{ \langle t_{pi}, P_{pri} \rangle; i = \overline{1, n_{пр}} \right\}, \quad (5)$$

где

t_{pi} - время (суммарная наработка) проведения i -го ПР;

P_{pri} - объем i -го ПР, определяемый относительной долей (процентом) заменяемых элементов;

$n_{\text{пр}}$ - число ПР, которые выполняются в течение заданного времени эксплуатации объекта T_3 .

Процент заменяемых элементов $P_{\text{пр}i}$ определяется следующим образом:

$$P_{\text{пр}i} = |E_{\text{пр}i}| \cdot 100 / |E_o|, \quad (6)$$

где

$E_{\text{пр}i}$ - подмножество элементов объекта, заменяемых при проведении ПР;

E_o - множество всех элементов объекта.

Прямые скобки $|E|$ в (6) обозначают число элементов (мощность) соответствующего множества E . Предполагается, что при определении $P_{\text{пр}i}$ в (6) в подмножество $E_{\text{пр}i}$ всегда включаются наименее надежные элементы из E_o ($E_{\text{пр}} \subset E_o$). Очевидно, что множество всех элементов объекта РЭТ может быть практически необозримым, поэтому необходимо уточнить, какие элементы включаются в E_o . Условимся, что в множество E_o включаются все элементы, которые учитываются при расчете показателя безотказности $\Omega(t)$ (то есть элементы, включаемые в структурную схему надежности объекта).

Вид функции $\Omega(t)$ на интервале времени после проведения i -го ПР зависит от всей предыстории процесса восполнения ресурса (от объема и времени выполнения всех ПР, проведенных до времени t). На интервале $(t_{\text{пр}1}, T_3]$ вид функции $\Omega(t)$ зависит от объема ПР $P_{\text{пр}1}$, выполненного в момент времени $t_{\text{пр}1}$, на интервале $(t_{\text{пр}2}, T_3]$ – от объемов ПР $P_{\text{пр}1}$ и $P_{\text{пр}2}$, выполнявшихся в моменты времени $t_{\text{пр}1}$ и $t_{\text{пр}2}$, и т.д. В общем случае будем записывать:

$$\Omega(t) = \Omega(t / \Psi(t)),$$

где $\Psi(t)$ - начальный отрезок, процесса Ψ , предшествующего моменту времени t :

$$\Psi(t) = \left\langle t_{\text{пр}i}, P_{\text{пр}i} \right\rangle; \forall i: t_{\text{пр}i} < t. \quad (7)$$

Функцию $\Omega(t / \Psi(t))$ можно представить как объединение (сумму) функций $\Omega_i(t / \Psi)$:

$$\Omega(t / \Psi) = \sum_{i=1}^{n_{\text{пр}}(t)} \Omega_i(t / \Psi), \quad (8)$$

где $\Omega_i(t / \Psi)$ - функция параметра потока отказов, которая определена только на i -м межремонтном интервале $(t_{\text{пр}i-1}, t_{\text{пр}i}]$ ($i = \overline{1, n_{\text{пр}}(t)}$, где $n_{\text{пр}}(t)$ - один из параметров процесса Ψ). Зависимость Ψ от t в (8) опущена для краткости записи, далее предполагается, что процесс Ψ определен на том же интервале, на каком определена функция $\Omega(t / \Psi)$.

Оптимизация параметров процесса выполнения ресурса

Восполнение ресурса объектов РЭТ не является самоцелью, ресурс восполняется для поддержания требуемого уровня надежности объектов в процессе их эксплуатации. Проведение ПР требует существенных экономических затрат, поэтому необходимо, во-первых, принять решение о необходимости ПР в принципе и, во-вторых, определить оптимальные параметры процесса выполнения ресурса Ψ , если проведение ПР признано необходимым. Задачу определения оптимальных параметров процесса Ψ в общем виде определим следующим образом:

$$T_0(\Psi^*) \geq T_0^{\text{тп}}, \quad (9 \text{ а})$$

$$c_{\Psi}(\Psi^*) \rightarrow \min, \quad (9 \text{ б})$$

где

Ψ^* - искомый оптимальный процесс выполнения ресурса;

$T_0(\Psi^*)$ - зависящая от процесса Ψ^* средняя наработка на отказ объекта;

$T_0^{\text{тп}}$ - требуемое значение средней наработки на отказ;

$c_{\Psi}(\Psi^*)$ - средняя удельная стоимость эксплуатации объекта при реализации процесса Ψ^* .

Средняя наработка на отказ $T_0(\Psi)$ с функцией $\Omega(t/\Psi)$ связана соотношением:

$$T_0(\Psi) = 1/\bar{\Omega}(\Psi), \quad (10)$$

где

$$\bar{\Omega}(\Psi) = \sum_{i=1}^{n_{\text{пр}}} \frac{1}{t_{\text{pi}} - t_{\text{pi-1}}} \int_{t_{\text{pi-1}}}^{t_{\text{pi}}} \Omega_i(t/\Psi) dt \quad (11)$$

Удельная стоимость эксплуатации $c_{\Psi}(\Psi)$ определяется как сумма

$$c_{\Psi}(\Psi) = c_{\text{отк}}(\Psi) + c_{\text{пр}}(\Psi), \quad (12)$$

где $c_{\text{отк}}(\Psi)$ и $c_{\text{пр}}(\Psi)$ - составляющие стоимости, приходящиеся на восстановление текущих отказов и ПР, которые определяются следующим образом:

$$c_{\text{отк}}(\Psi) = \frac{1}{T_{\Psi}} \sum_{j \in E_0} (C_{\text{зам } j} + C_{0j}) n_{\text{отк } j}(\Psi); \quad (13)$$

$$c_{\text{пр}}(\Psi) = \frac{1}{T_{\Psi}} \sum_{i=1}^{n_{\text{пр}}} C_{\text{пр } i}(\Psi), \quad (14)$$

где

$C_{\text{зам } j}$ - стоимость операции замены j -го элемента;

C_{0j} - стоимость j -го элемента;

$n_{\text{отк } j}(\Psi)$ - среднее число отказов j -го элемента на интервале T_{Ψ} , зависящее от процесса Ψ ;

$C_{np i}(\Psi)$ - стоимость i -го ПР ($i = \overline{1, n_{np}}(t)$).

С учетом определения процесса Ψ (5) понятно, что задача (9) не может быть решена классическими стандартными методами оптимизации. Главная трудность состоит в том, что элементы решения – пары $\langle t_{pi}, P_{np i} \rangle$, являются зависимыми, так как выбор оптимальных параметров каждого последующего ПР зависит от выбранных ранее параметров всех предыдущих ПР. Кроме того, число всех ПР n_{np} (число элементов решения) изменяется в зависимости от выбираемых параметров $\langle t_{pi}, P_{np i} \rangle$. С учетом этого остается надеяться решить задачу (9) только приближенно.

Предлагается следующий подход к решению задачи (9), включающий два этапа. На первом этапе определяется множество условно оптимальных решений $\Psi^+(P_{np})$, каждое из которых найдено из условия (9 а) при фиксированном значении P_{np} . В результате будет получено множество таких решений $\{\Psi^+(P_{np})\}$ для некоторого количества значений $P_{np} \in (0, 100\%)$. Для каждого значения P_{np} находится также соответствующая решению $\Psi^+(P_{np})$ удельная стоимость эксплуатации $c_{\varepsilon}(\Psi^+(P_{np}))$. Таким образом, по результатам первого этапа может быть построен график зависимости удельной стоимости эксплуатации c_{ε} от объема ПР P_{np} , вид которого примерно такой, как это показано на рис. 3.

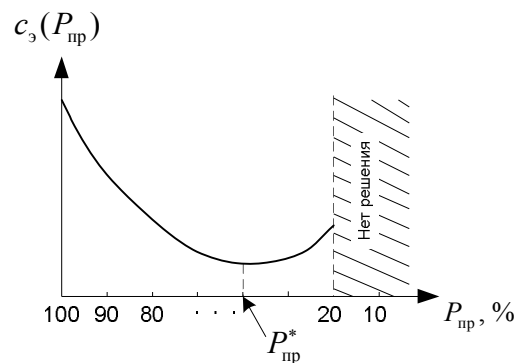


Рис. 3. Определение оптимального значения P_{np}^* .

Каждая точка этого графика соответствует условно оптимальному решению $\Psi^+(P_{np})$, полученному при фиксированном значении P_{np} . Расчеты при поиске условно оптимальных решений целесообразно производить в последовательности убывания значений P_{np} , начиная с максимальных значений. Такая последовательность рекомендуется потому, что условно оптимальное решение $\Psi^+(P_{np})$ всегда существует при $P_{np} = 100\%$, а при убывании величины P_{np} при некотором ее малом значении решения может не быть (при малом объеме ремонта требование (9 а) может не выполняться ни при каком малом значении межремонтного ресурса). Из физических соображений очевидно, что должен существовать минимум графика $c_{\varepsilon}(P_{np})$ при некотором значении P_{np}^* .

На втором этапе производится анализ графика $c_3(P_{np})$ и выбор оптимального объема ремонта P_{np}^* , при котором обеспечивается минимальная удельная стоимость эксплуатации $c_3(P_{np}^*)$ (выполняется условие (9 б)). Соответствующее значению P_{np}^* условно оптимальное решение $\Psi^+(P_{np}^*)$ принимается в качестве приближенного решения задачи.

Очевидно, что в рассмотренной схеме решения задачи (9) основные вычисления производятся на первом этапе, при формировании условно оптимальных решений $\Psi^+(P_{np})$. Поэтому целесообразно рассмотреть алгоритм формирования условно оптимального решения.

Алгоритм формирования условно оптимального решения

Структурная схема алгоритма приведена на рис. 4. Для получения функции $\Omega(t)$ заданный интервал эксплуатации T_3 разбивается на равные интервалы Δt . Функция $\Omega(t)$ получается путем статистического моделирования отказов объекта в заданных интервалах. Величина Δt выбирается с учетом следующих противоречивых факторов. При уменьшении величины Δt :

1. увеличивается точность определения прогнозируемых сроков проведения ПР;
2. уменьшается точность оценки функции $\Omega(t)$ в интервале Δt ;
3. возрастают затраты машинного времени на моделирование.

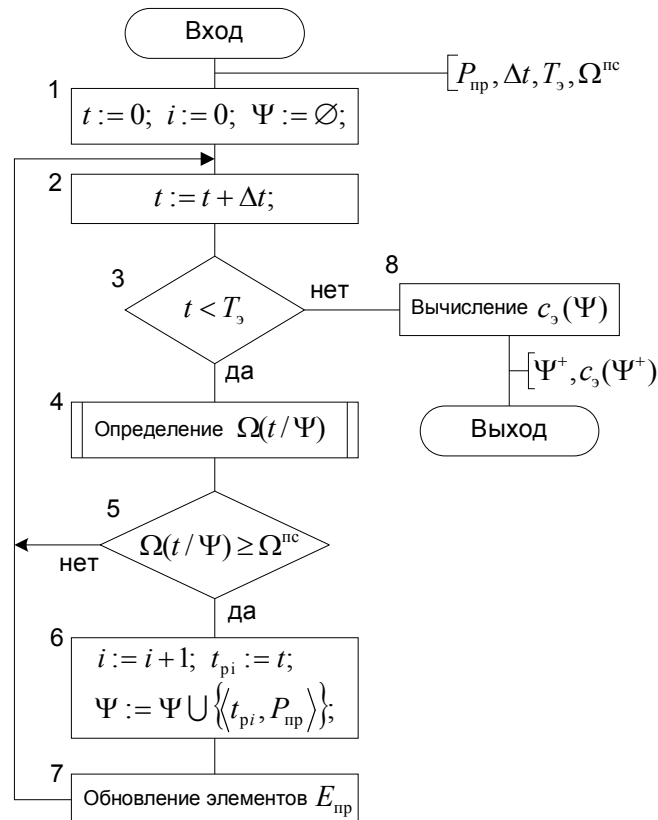


Рис. 4. Алгоритм формирования условно оптимального процесса Ψ^+ .

Исходной информацией являются заданные значения P_{np} , Δt , T_g и Ω^{nc} . Алгоритм, показанный на рис. 4, по сути, имитирует процесс восполнения ресурса объекта на заданном интервале эксплуатации T_g .

Оператором 1 устанавливаются начальные значения переменных: t – текущее модельное время, изменяемое с интервалом Δt ; i – количество выполненных ПР. Кроме того, оператором 1 создается структура данных, в которой будет сохраняться информация о процессе Ψ . Вначале структура Ψ пуста.

Оператор 2 формирует очередное значение модельного времени t . Оператор 3 проверяет, не вышло ли время t за пределы заданного интервала T_g . Оператор 4 формирует оценку функции $\Omega(t/\Psi)$ в текущем интервале $(t - \Delta t, t]$ с учетом выполненной к данному времени части процесса $\Psi(t)$. Оператор 5 проверяет выполнение условия наступления ПС. Если ПС не достигнуто, процесс моделирования продолжается (циклически повторяется выполнение операторов 2-5). Если при выполнении оператора 5 оказывается, что критерий наступления ПС удовлетворяется, то выполняются операторы 6 и 7. Оператором 6 выполняются следующие действия:

- определяется номер i текущего ПР (выполняемого в момент времени t);
- определяется время выполнения i -го ПР t_{pi} ;
- формируется пара (элемент решения) $\langle t_{pi}, P_{np} \rangle$, которая добавляется в структуру Ψ .

Оператор 7 имитирует выполнение ПР с параметрами $\langle t_{pi}, P_{np} \rangle$. Для этого в статистической модели, с помощью которой формируется функция $\Omega(t/\Psi)$, производится перепланирование отказов всех элементов объекта, которые заменяются при проведении ПР (этим имитируется их обновление). Множество таких элементов E_{np} с учетом (6) определяется из уравнения

$$|E_{np}| \cong \lfloor |E_o| \cdot P_{np} / 100 \rfloor_{ц},$$

где скобки $\lfloor \rfloor_{ц}$ в правой части обозначают операцию взятия целой части.

После выполнения операторов 6 и 7 далее работа алгоритма продолжается описанным выше образом.

Если текущее модельное время t достигнет заданного ограничения T_g , то оператор 3 передаст управление оператору 8, который вычисляет оценку удельной стоимости эксплуатации $c_g(\Psi)$. На этом работа алгоритма завершается. В структуре данных Ψ будут сохранены параметры условно оптимального процесса восполнения ресурса Ψ^+ .

Реализация модели

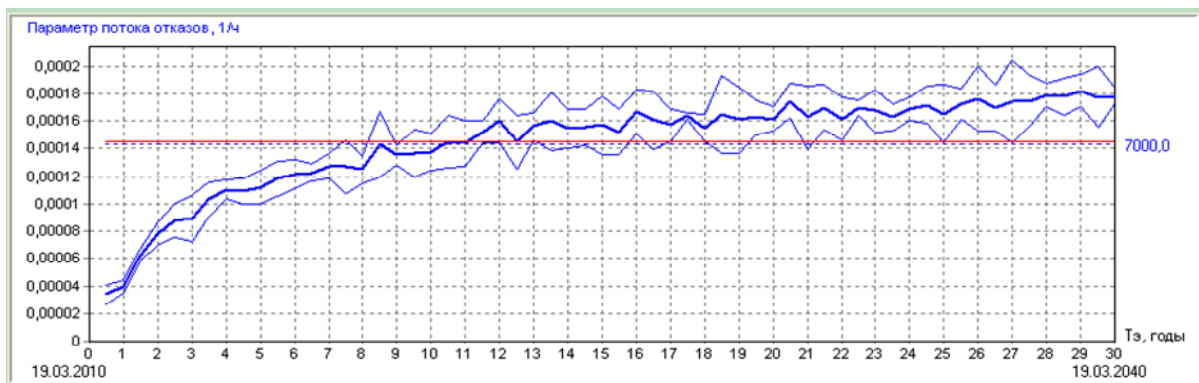
Рассмотренная теоретическая модель оптимизации процесса восполнения ресурса реализована программно на базе имитационной статистической модели, с помощью которой получается оценка функции $\Omega(t/\Psi)$. Некоторые общие сведения об этой модели приведены в [3]. Все программное обеспечение разработано в системе программирования Delphi. В рамках данной статьи у нас нет возможности рассмотреть детали программной реализации, поэтому приведем только пример основных результатов, получаемых с помощью разработанной модели.

На рис. 5 показан вид функции $\Omega(t/\Psi)$, полученной для тестового объекта РЭТ, взятого нами для примера. Объект состоит из последовательно соединенных (в смысле

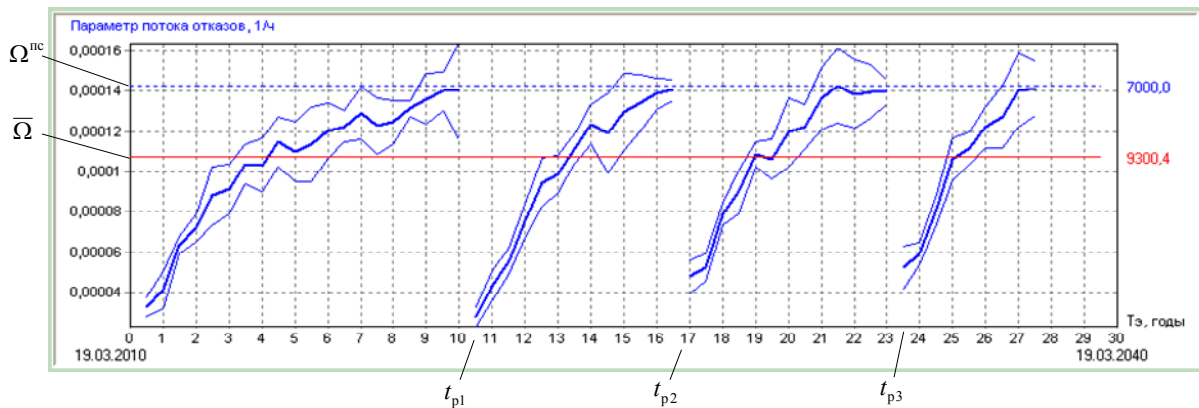
надежности) 50 элементов, имеющих различную надежность. Отказы всех элементов подчинены DN -распределению с коэффициентом вариации 0.8 [4]. Продолжительность эксплуатации объекта задана равной $T_0 = 30$ лет.

Средний график (жирная линия) является оценкой параметра потока отказов в интервалах $\Delta t = 3$ мес., верхний и нижний графики представляют границы 95%-го доверительного интервала.

На рис. 5 а представлен график функции $\Omega(t/\Psi)$, полученный для случая, если ПР не проводятся ($\Psi = \emptyset$). Средняя наработка на отказ объекта в этом случае равна $T_0 \approx 6960$ ч (это соответствует величине $\bar{\Omega} = 1/T_0 \approx 0.000144$ 1/ч). На рис. 5 б показана та же функция в случае, если ПР проводятся в моменты времени наступления ПС, определяемого по критерию (1) при заданном для примера фиксированном значении процента замены элементов $P_{пр} = 40\%$.



а



б

Рис.5. Примеры графиков функции $\Omega(t/\Psi)$: а – ПР не проводятся; б – ПР проводятся

В качестве граничного значения параметра потока отказов задана величина $\Omega^{nc} = 1/T_0^{mp} = 1/7000$ ч = 0.000143 1/ч. По графикам рис. 5 б видно, как за счет проведения ПР среднее за время эксплуатации T_0 значение параметра потока отказов уменьшилось до величины $\bar{\Omega} \approx 0.000107$ 1/ч, что соответствует увеличению средней наработки на отказ до значения $T_0 = 1/\bar{\Omega} \approx 9300$ ч.

Полученные в результате моделирования моменты времени ПР t_{pi} (совместно с заданным значением $P_{пр}$) образуют процесс $\Psi^+(P_{пр})$, параметры которого являются условно оптимальным решением задачи (9) (оптимальным при условии фиксированного значения $P_{пр}$). На рис. 6 показан график значений стоимости эксплуатации $c_э(P_{пр})$, полученных при различных значениях $P_{пр}$. За счет стохастичности моделируемого процесса величины t_{pi} могут изменяться от сеанса к сеансу моделирования, поэтому оценки $c_э(P_{пр})$ также могут изменяться. На рис. 6 показаны графики для среднего значения $\bar{c}_э(P_{пр})$ (жирная линия) и верхних и нижних границ доверительного интервала, равного двойному среднему квадратическому отклонению. По графику $\bar{c}_э(P_{пр})$ находится приближенное оптимальное значение процента замены элементов $P_{пр}^*$.



Рис. 6. Определение оптимального значения $P_{пр}^*$.

Выводы

Предложенная теоретическая модель процесса восполнения ресурса сложного объекта РЭТ позволяет прогнозировать возможный его характер еще на этапе разработки объекта. На основе такого прогноза оказывается возможным 1) принимать прогнозное решение о необходимости ПР для объектов РЭТ данного типа, и 2) заблаговременно определять оптимальные параметры ПР в случае, если принято решение об их необходимости.

Список литературы

1. ГОСТ 27.002-89. Надежность в технике. Основные понятия. Термины и определения. Введ. с 01.07.1990.
2. ДСТУ 2860-94. Надійність техніки. Терміни та визначення.

3. Ленков С.В., Боряк К.Ф., Браун В.О., Банзак Г.В., Цыцарев В.Н. Имитационная статистическая модель процесса технического обслуживания и ремонта сложных объектов радиоэлектронной техники // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К., 2012. – № 38. – С.63 – 69.
4. ГОСТ 27.005-97. Надежность в технике. Модели отказов. Основные положения. – Введ. 01.01.99. – 45 с.

МОДЕЛЮВАННЯ І ОПТИМІЗАЦІЯ ПРОЦЕСУ ЗАПОВНЕННЯ РЕСУРСУ СКЛАДНИХ ОБ'ЄКТІВ РАДІОЕЛЕКТРОННОЇ ТЕХНІКИ

К.Ф. Боряк¹, С.В. Ленков², В.М. Цицарев²

¹ Одеська державна академія технічного регулювання та якості,
вул. Ковальська 15, Одеса, 65020, Україна

² Військовий інститут Київського національного університету імені Тараса Шевченка,
вул. Ломоносова, 81, Київ, 03680, Україна, e-mail: lenkov_s@ukr.net

У статті проведено моделювання і оптимізацію процесу заповнення ресурсу складних об'єктів радіоелектронної техніки. Пропонується критерій для визначення ресурсу відновлюваних об'єктів РЕТ. Вводиться поняття процесу заповнення ресурсу об'єктів РЕТ і формулюється завдання його оптимізації. Розроблений новий алгоритм визначення оптимальних параметрів цього процесу.

Ключові слова: радіоелектронна техніка, технічний об'єкт, ресурс.

MODELING AND OPTIMIZATION OF THE OPERATIONAL LIFE EXTENSION PROCESS FOR COMPLEX RADIOELECTRONIC SYSTEMS

K. Boryak¹, S.Lenkov², V. Cicarev²

¹ Odessa state academy of the technical adjusting and quality,
15 Kovalskaya str., Odessa, 65020, Ukraine

² Military Institute, Taras Shevchenko National University of Kyiv,
81 Lomonosov str., Kyiv, 03680, Ukraine; e-mail: lenkov_s@ukr.net

Modeling and optimization of the operational life extension process for complex radioelectronic systems was performed in this work. A criterion to determine the operational life of restorable radioelectronic systems was proposed. A phenomenon of the operational life extension process for radioelectronic systems was established and the problem of optimization of this process was formulated. A new algorithm to determine the optimum parameters of the process was developed.

Keywords: radioelectronic system, technical asset, operational life.

ІНФОРМАЦІЙНА МОДЕЛЬ БЕЗПЕКИ ТЕХНОЛОГІЙ ЗВ'ЯЗКУ

В.Б. Дудикевич¹, В.О. Хорошко², Г.В. Микитин¹, Р.І. Банах¹, А.І. Ребець¹

¹ Національний університет «Львівська політехніка»,
вул. С. Бандери, 12, Львів-13, 79013, Україна,

² Національний авіаційний університет,
пр. Космонавта Комарова, 1, Київ, 03058, Україна; e-mail: professor_va@ukr.net

Запропоновано інформаційну модель захисту даних в технологіях зв'язку GSM, PSTN, VoIP, ADSL, Wi-Fi на рівні системи "об'єкт - загроза - захист".

Ключові слова: об'єкт захисту, загроза інформаційній безпеці, технологія захисту інформації

Інформаційна модель захисту даних в технологіях зв'язку: GSM, PSTN, VoIP, ADSL, Wi-Fi

Захист даних в інформаційно-телекомунікаційних системах – один з основних сегментів Національної програми інформатизації та Концепції технічного захисту інформації в Україні [1, 2]. Триває розвиток нових методів захисту інформації та удосконалення відомих засобів забезпечення безпеки телекомунікаційних систем. Зокрема, в літературі [3] розглянуто принципи побудови систем зв'язку, стандарти та загрози інформаційній безпеці. В роботі [4] запропоновано методику систематизації та представлення експертних знань про комплексні системи захисту інформації, яка забезпечує оцінювання захищеності інформаційних систем та забезпечення рівнів безпеки. В роботі [5] представлено принципи створення захищених мереж стільникового зв'язку, розглянуто заходи та засоби забезпечення якості передавання інформації.

З метою забезпечення цілісної безпеки структури “система – канал зв'язку– система” розглянемо інформаційну модель захисту даних в технологіях голосової телефонії та передавання даних (рис. 1). Модель створена на основі принципів системного аналізу – ієрархічності, багатоаспектності, цілісності і характеризує безпеку технологій GSM, PSTN, VoIP, ADSL, Wi-Fi на рівні системи “об'єкт – загроза – захист”. На основі інформаційної моделі формується комплекс уніфікованих методів і засобів забезпечення безпеки даних в технологіях зв'язку відповідно до нормативного забезпечення.

Технологія GSM: характеристика системи “об'єкт – загроза – захист”.

Технологія GSM (Global System for Mobile Communications) – глобальний цифровий стандарт для мобільного стільникового зв'язку з розділенням частотного каналу за принципом TDMA та середнім ступенем безпеки. Технологія GSM відноситься до мереж 2-го покоління (2G – цифровий стільниковий зв'язок), хоча з 2010 р. умовно знаходилась у фазі 2.75G завдяки численним розширенням. Технологія GSM функціонує в чотирьох частотних діапазонах: 850 МГц, 900 МГц, 1800 МГц, 1900 МГц. Загальна архітектура технології GSM представлена на рис. 2.

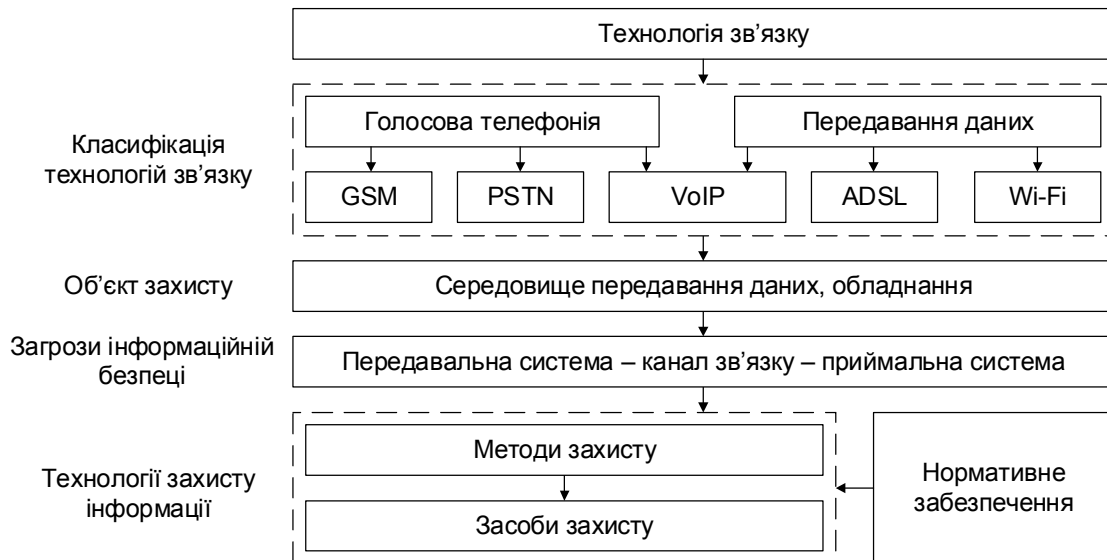


Рис. 1. Інформаційна модель захисту даних в технологіях зв'язку

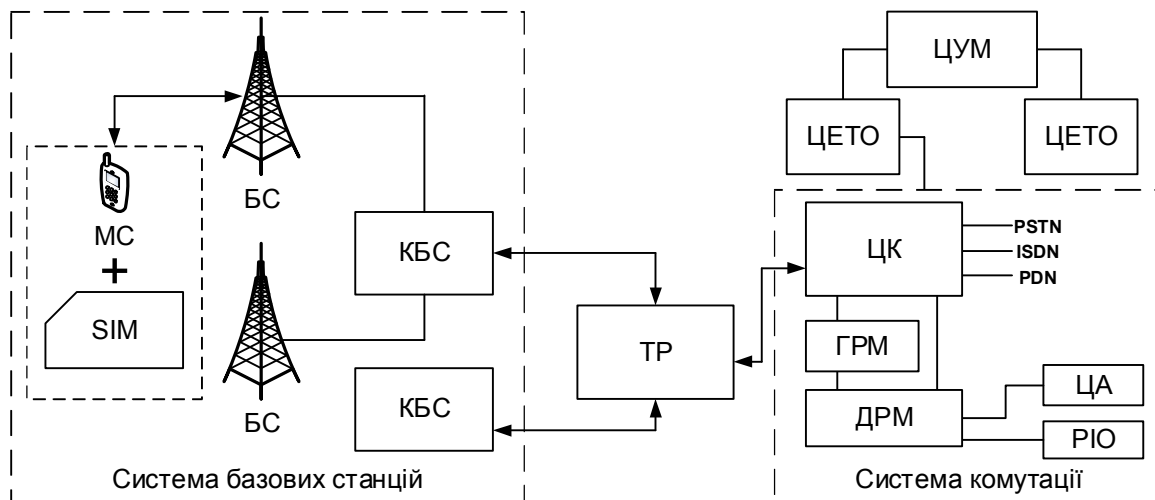


Рис. 2. Загальна архітектура технології GSM

Мобільна станція (МС) із мікропроцесорною картою SIM (Subscriber Identify Modul), в яку занесені унікальні дані для обміну інформацією між абонентами. Контролери базових станцій (КБС) – здійснюють керування базовими станціями (БС) і в подальшому формують з'єднання з центром комутації (ЦК), за допомогою якого можна створити канал передавання даних між двома абонентами. Трансcoder (ТР), як проміжна ланка між БС та системою комутації, забезпечує перетворення вихідних сигналів каналу передавання мовного сигналу і даних (64 Кбіт/с) до виду, що відповідає рекомендаціям GSM по радіоінтерфейсу (13 Кбіт/с). В домашньому реєстрі місцезнаходження (ДРМ) зберігається інформація про місцезнаходження будь-якої МС, яка дозволяє центру комутації реалізувати виклик до цієї станції.

Загалом ДРМ представляє базу даних (БД), в якій зберігається службова інформація про абонента. Гостьовий реєстр місцезнаходження (ГРМ) – це тимчасова БД абонентів, які знаходяться в зоні дії відповідного центру комутації. У кожного ЦК є лише один гостьовий реєстр місцезнаходження. В ГРМ зберігається та ж інформація

що і в ДРМ, але лише до того часу доки МС знаходиться в зоні дії цього ГРМ. Центр автентифікації (ЦА) – це сервіс, за допомогою якого перевіряється право на доступ абонента до мережі, зокрема формуються ключі та алгоритми автентифікації. В ЦА зберігаються: унікальні номери абонента, індивідуальний ключ, алгоритм автентифікації. Реєстр ідентифікації обладнання (РІО) – сервіс, в якому знаходиться централізована БД для підтвердження міжнародного ідентифікаційного номеру МС (IMEI). Центр експлуатації технічного обслуговування (ЦЕТО) – забезпечує контроль і керування іншими компонентами мережі та контроль якості її роботи. Центр управління мережею (ЦУМ) – дозволяє забезпечити раціональне ієрархічне управління мережею GSM та відповідає за експлуатацію і технічне обслуговування.

В GSM використовується дві смуги частот: uplink (трансмсія вгору) 890 – 915 МГц, яка призначена для передавання даних від МС до БС; downlink (трансмсія вниз) 935 – 960 МГц відповідно для передавання інформації від БС до МС. Кожна із смуг дозволяє організувати по 124 симплексних канали із частотним рознесенням між каналами до 200 кГц.

Враховуючи архітектуру, функціонування та особливості технології GSM розглянемо характеристику системи “об’єкт – загроза – захист” згідно інформаційної моделі (рис. 1) (табл. 1) [6, 7, 8].

Технологія PSTN: характеристика системи “об’єкт – загроза – захист”.

Технологія PSTN (Public Switched Telephone Network) – це телефонна мережа загального користування (ТМЗК), для доступу до якої використовуються: проводові телефонні апарати, автоматичні телефонні станції (АТС), обладнання передавання даних. Передавання сигналів, налаштування з’єднання, розмова в технології PSTN реалізуються через універсальну лінію зв’язку від АТС джерела до АТС адресата з особливістю встановлення зв’язку між абонентами за умови розмови двох (рис. 3).

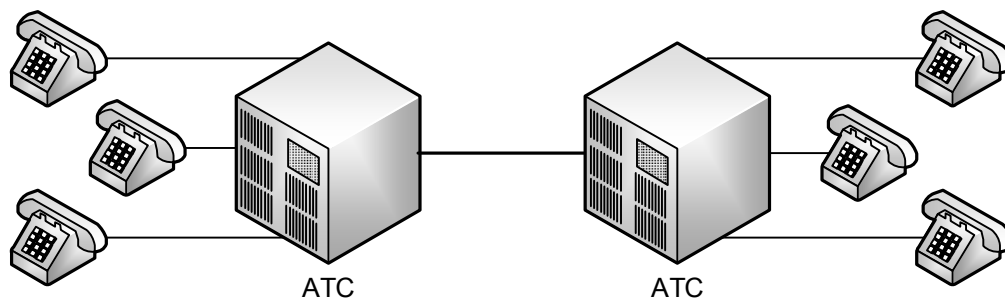


Рис. 3. Загальна архітектура технології PSTN

Технологія PSTN нормативно забезпечена стандартами Міжнародного союзу електрозв’язку (ITU-T) і на практиці здебільшого реалізується за зіркоподібною топологією. Поєднання взаємопов’язаних мереж (стандарт E.163 для ТМЗК) і єдиний міжнародний телекомунікаційний план нумерації (рекомендація E.164) дозволяють будь-якому абоненту у глобальному адресному просторі набрати телефонний номер будь-якого іншого абонента. Інформація в мережах такого типу передається зі швидкістю до 33.6 Кб/с.

На основі інформаційної моделі (рис. 1) розглянемо характеристику системи “об’єкт – загроза – захист” для технології PSTN, враховуючи її особливості (табл. 2) [6, 9].

Таблиця 1.

Технологія GSM та її характеристика

GSM		Характеристики системи "об'єкт-загроза-захист"
Об'єкт: середовище передавання даних, обладнання		Ефір: ▪ Мобільна станція ▪ Базові (передавально-приймальні) станції ▪ Провідне середовище, або ефір: ▪ Контролер базових станцій ▪ Транскодер ▪ Центр комутації ▪ "Домашній" реєстр місцезнаходження ▪ "Гостьовий" реєстр місцезнаходження ▪ Центр автентифікації ▪ Реєстр ідентифікації обладнання ▪ Центр експлуатації і технічного обслуговування ▪ Центр управління мережею
Загрози інформаційній безпеці		▪ Знищення або викривлення логічної структури даних ▪ Несанкціоноване отримання інформації та її модифікація ▪ Зашумлення каналу зв'язку
Захист інформації: технології	Методи	▪ Шифрування даних в радіоканалі ▪ Автентифікація повідомлень ▪ Автентифікація користувача ▪ Перепризначення TMSI ▪ Ідентифікація обладнання
	Засоби	▪ Скремблери ▪ Криптофони ▪ Інвертори спектру ▪ Генератори шуму ▪ Змінювачі голосу ▪ SIM-карти ▪ Шифратори ▪ Алгоритми шифрування (A5/1, A5/2, A5/3) ▪ Ідентифікаційний номер рухомого терміналу (IMEI)

Технологія VoIP: система "об'єкт – загроза – захист"

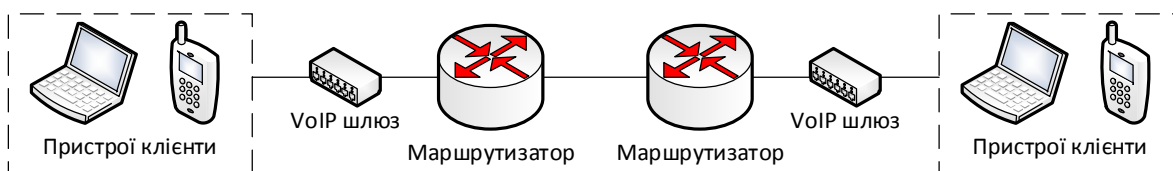
Технологія VoIP (Voice over IP) – технологія передавання медіа-даних в режимі реального часу за допомогою системи протоколів TCP/IP. В технології VoIP аналоговий мовний сигнал від одного абонента дискретизується (кодується), здійснюється компресія та передавання цифровими каналами зв'язку до іншого абонента, де проводиться зворотна операція – декомпресія, декодування і відтворення аналогового сигналу. У випадку, якщо дзвінок надходить на іншу технологію, наприклад PSTN чи GSM, то сигнал проходить через IP-шлюз, який перетворює цифровий (VoIP) сигнал в аналоговий. Для передавання голосу через IP-мережу відбувається процедура стискання сигналу спеціальною програмою-кодеком. Це здійснюється для збільшення швидкості передавання даних відповідно для підвищення якості зв'язку. Рівень безпеки передавання мовної інформації підвищує процедура шифрування даних. Зв'язок між двома VoIP-терміналами можливий лише за

умови сумісних кодеків. З'єднання двох VoIP-терміналів між собою в мережі забезпечується підтримкою однакового протоколу комутації, наприклад SIP (рис. 4).

Таблиця 2.

Технологія PSTN та її характеристика

PSTN		Характеристики системи "об'єкт-загроза-захист"
Об'єкт: середовище передавання даних, обладнання		Провідне середовище: ▪ Обладнання провайдера – АТС – Комутатори ▪ Пристрої клієнти – Телефонні апарати
Загрози інформаційній безпеці		▪ Застосування закладних пристроїв для перехоплення телефонних повідомлень ▪ Перехоплення акустичних коливань з пристроїв, які володіють "мікрофонним ефектом" ▪ Високочастотне нав'язування ▪ Прослуховування приміщень за допомогою виносних мікрофонів ▪ Перехоплення побічних електромагнітних сигналів випромінювання і наведень
Захист інформації: технології	Методи	▪ Контроль параметрів абонентської телефонної лінії (АТЛ) у робочому стані: – Контроль напруги живлення – Контроль струму короткого замикання – Контроль навантажувальної характеристики – Виявлення сторонніх сигналів ▪ Контроль параметрів знеструмлених АТЛ: – Вимірювання опору шлейфа – Вимірювання омичної асиметрії – Вимірювання параметрів імпедансу АТЛ – Контроль вольт-амперної характеристики – Контроль лісажу-характеристики – Контроль перехідної характеристики ▪ Послаблення корисного сигналу ▪ Фільтрація
	Засоби	▪ Засоби контролю АТЛ: – Сторожові – Пошукові – Універсальні ▪ Засоби закриття мовного сигналу: – Скремблери – Маскувальники – Вокодери ▪ Нелінійні атенюатори ▪ Загороджувальні фільтри

**Рис. 4.** Загальна архітектура технології VoIP

При передаванні даних в IP-мережах використовуються різні алгоритми стиснення мовної інформації, наприклад стиснення голосового потоку у 8 і більше разів, а деякі з них практично залишають сигнал на рівні імпульсно-кодової модуляції (64 кбіт/с).

На основі інформаційної моделі (рис. 1) розглянемо характеристику системи “об’єкт – загроза – захист” для технології VoIP, враховуючи її особливості (табл. 3) [6, 10].

Таблиця 3.

Технологія VoIP та її характеристика

VoIP		Характеристики системи "об'єкт-загроза-захист"
Об'єкт: середовище передавання даних, обладнання		Провідне середовище, або ефір: - Мережеві пристрої - Маршрутизатор - VoIP шлюз - Пристрої клієнти - VoIP телефон / ПК з VoIP програмним забезпеченням
Загрози інформаційній безпеці		- Відмова в обслуговуванні (DoS) - Крадіжка реєстраційних даних і маніпуляція ними - Атаки на систему автентифікації - Підміна (спуфінг) Caller ID - Атаки типу "man in the middle" - Атаки типу "Vlan hopping" - Спам через Інтернет-телефонію (SPIT) - VoIP фішинг (Vishing)
Захист інформації: технології	Методи	- Ідентифікація/ авторизація користувачів - Перевірка обладнання на право доступу до мережі - Шифрування даних - Забезпечення цілісності - Контроль авторизованих абонентів - Окремий Інтернет-канал для VoIP
	Засоби	- Системи виявлення/ запобігання атак - Віртуальні приватні мережі - Брандмауер VoIP - Захищені мережеві протоколи - Міжмережеві екрани - Системи контролю цілісності

Технологія ADSL: система “об’єкт – загроза – захист”

Технологія ADSL (Asymmetric Digital Subscriber Line) – технологія широкосмугового доступу, яка забезпечує передавання швидкісного цифрового сигналу звичайною аналоговою телефонною лінією за умови одночасного користування телефоном та Інтернетом. Технологія ADSL відноситься до класу широкосмугових (broadband) та передбачає організацію асиметричного обміну даними (рис. 5).

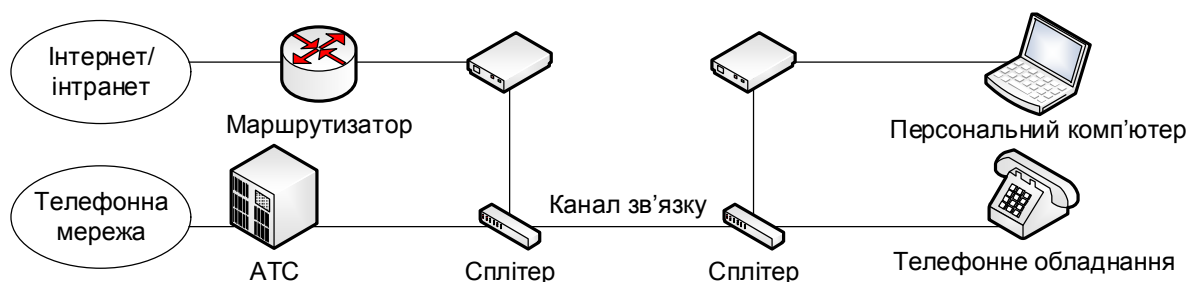


Рис. 5. Загальна архітектура технології ADSL

Технологія забезпечує швидкість передавання даних в напрямку абонента – 24 Мбіт/с, від абонента – 3.5 Мбіт/с. В ADSL мовний сигнал передається в частотному діапазоні 0.3 – 3.4 кГц, а інформація в діапазоні 26 кГц – 1104 МГц, який розділений на два піддіапазони: 26 – 138 кГц (для вихідного потоку даних); 138кГц – 1.1МГц (для вхідного). Особливістю технології ADSL є можливість одночасно працювати в Інтернет і розмовляти телефоном.

На основі інформаційної моделі (рис. 1) розглянемо характеристику системи “об’єкт – загроза – захист” для технології ADSL, враховуючи її особливості (табл. 4) [11].

Технологія Wi-Fi: система “об’єкт – загроза – захист”

Технологія WI-FI (Wireless Fidelity) – технологія об’єднує декілька протоколів і ґрунтується на системі стандартів IEEE 802.11. На практиці широко використовується протокол IEEE 802.11n, який визначає принцип функціонування безпроводних мереж (рис. 6).



Рис. 6. Загальна архітектура технології Wi-Fi

Таблиця 4.

Технологія ADSL та її характеристика

ADSL		Характеристики системи "об'єкт-загроза-захист"
Об'єкт: середовище передавання даних: обладнання		Провідне середовище: ▪ Мережеві пристрої – ADSL модеми – Сплітери ▪ Пристрої клієнти
Загрози інформаційній безпеці		▪ Відмова в обслуговування (DoS) ▪ Крадіжка реєстраційних даних і маніпуляція ними ▪ Атаки на систему автентифікації ▪ Атаки типу "man in the middle" ▪ Несанкціонована модифікація лінії зв'язку
Захист інформації: технології	Методи	▪ Ідентифікація ▪ Автентифікація ▪ Перевірка обладнання на право доступу до мережі ▪ Послаблення корисного сигналу ▪ Фільтрація
	Засоби	▪ Системи ідентифікації/ автентифікації користувачів ▪ Системи виявлення/ запобігання атак ▪ Віртуальні приватні мережі ▪ Брандмауери; ▪ Системи контролю цілісності ▪ Нелінійні атенюатори ▪ Загороджувальні фільтри

Функціонування технології Wi-Fi полягає у підключенні мобільного пристрою до точки доступу, роль якої може виконувати як окремий пристрій, так і мобільний, при правильному налаштуванні. Точка доступу розповсюджує свій ідентифікатор (SSID) в ефір за допомогою спеціальних сигналів ("маячків").

На сьогодні в Україні функціонують стандарти: IEEE 802.11a (діапазон частот 5.170 – 5.905 ГГц, максимальна швидкість передавання інформації 54 Мбіт/с), IEEE 802.11b (діапазон частот 2.4 – 2.5 ГГц, максимальна швидкість передавання інформації 11 Мбіт/с), IEEE 802.11g (діапазон частот 2.4 – 2.5 ГГц, максимальна швидкість передавання інформації 54 Мбіт/с), IEEE 802.11n (діапазон частот 2.4 – 2.5 ГГц та 5.170 – 5.905 ГГц, максимальна швидкість передавання інформації 320 Мбіт/с); впроваджується IEEE 802.11ac (максимальна швидкість передавання інформації більше 1 Гбіт/с).

На основі інформаційної моделі (рис. 1) розглянемо характеристику системи "об'єкт – загроза – захист" для технології Wi-Fi, враховуючи її особливості (табл. 5) [12, 13, 14].

Таблиця 5.

Технологія Wi-Fi та її характеристика

Wi-Fi		Характеристики системи "об'єкт-загроза-захист"
Об'єкт: середовище передавання даних, обладнання		Ефір: - Базова станція - Маршрутизатор / безпроводна точка доступу - Клієнтські пристрої - Мобільний пристрій з модулем Wi-Fi
Загрози інформаційній безпеці		- Відмова в обслуговування (DoS) - Крадіжка реєстраційних даних і маніпуляція ними - Атаки на систему автентифікації - Спуфінг - Атаки типу "man in the middle" - Несанкціоноване отримання інформації та її модифікація.
Захист інформації: технології	Методи	- Ідентифікація/авторизація користувачів - Перевірка обладнання на право доступу до мережі - Приховування ідентифікатора мережі - Шифрування даних - Забезпечення цілісності - Обмеження доступу до центрального вузла - Контроль авторизованих абонентів
	Засоби	- Брандмауери - Базові системи автентифікації - Протоколи шифрування - Модель AAA (Authentication Authorization Accounting) - Системи виявлення/запобігання атак - Системи приманки - Системи контролю цілісності

Нормативне забезпечення системи "об'єкт – загроза – захист" для технологій зв'язку

На основі інформаційної моделі захисту мовної інформації в ІКТ (рис. 1) розглянемо елементи нормативного забезпечення системи "об'єкт – загроза – захист", що є основою застосування уніфікованих методів і засобів забезпечення безпеки передавання даних в тракті "система – канал зв'язку – система" (табл. 6).

Таблиця 6.

Нормативне забезпечення захисту мовної інформації в ІКТ

Закони та постанови	- Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 №80/94-ВР - Постанова Кабінету міністрів "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" від 29.03.2006 № 373. Остання редакція від 13.10.2011.
Стандарти	1. Захист інформації. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. – [Чинний від 1997-01-01] – К.: Держстандарт України, 1996 – 20 с. – (Державний стандарт України).

Продовження таблиці 6.

2. Захист інформації. Технічний захист інформації. Порядок проведення робіт: ДСТУ 3396.1-96. – [Чинний від 1997-07-01] – К.: Держстандарт України, 1996 – 4с. – (Державний стандарт України).
3. Захист інформації. Технічний захист інформації. Терміни та визначення: ДСТУ 3396.2-97. – [Чинний від 1998-01-01] – К.: Держстандарт України, 1997 – 6 с. – (Державний стандарт України).
4. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння: ДСТУ 4145-2002. – [Чинний від 2003-07-01]. – К.: Держспоживстандарт України, 2002. – 38 с. – (Національний стандарт України).
5. Інформаційні технології. Методи захисту. Геш-функції. Частина 1. Загальні положення (ISO/IEC 10118 – 1 : 2000, IDT): ДСТУ ISO/IEC 10118-1:2003. – [Чинний від 2005-01-01]. – К.: Держспоживстандарт України, 2003. – 10 с. – (Національний стандарт України).
6. Інформаційні технології. Методи захисту. Геш-функції. Частина 2. Геш-функції з використанням n-бітового блокового шифру (ISO/IEC 10118 – 2 : 2000, IDT): ДСТУ ISO/IEC 10118-2:2003. – [Чинний від 2005-01-01]. – К.: Держспоживстандарт України, 2003. – 24 с. – (Національний стандарт України).
7. Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 1. Загальні положення (ISO/IEC 14888-1:1998, IDT): ДСТУ ISO/IEC 14888-1-2002. – [Чинний від 2006-10-01]. – К.: Держспоживстандарт України, 2002. – 18 с. – (Національний стандарт України).
8. Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми на основі ідентифікаторів (ISO/IEC 14888 – 2 : 1999, ГОТ): ДСТУ ISO/IEC 14888-2-2002. – [Чинний від 2006-10-01]. – К.: Держспоживстандарт України, 2002. – 22 с. – (Національний стандарт України).
9. Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми на основі сертифікатів (ISO/IEC 14888 – 3 : 1998, IDT): ДСТУ ISO/IEC 14888-3-2002. – [Чинний від 2006-10-01]. – К.: Держспоживстандарт України, 2002. – 34 с. – (Національний стандарт України).
10. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий: ГОСТ Р ИСО/МЭК 13335-1-2006. – [Чинний від 2007-06-01]. – М.: Стандартиформ, 2007. – 23 с. – (Межгосударственный стандарт).
11. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.05.1999 №26: НД ТЗІ 2.5-001-99. – [чинний від 1999-07-01]. – К.: ДСТСЗІ СБ України, 1999 – 56 с. – (Нормативний документ).

Продовження таблиці 6.

	12. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.05.1999 №26: НД ТЗІ 2.5-002-99. – [чинний від 1999-07-01]. – К.: ДСТСЗІ СБ України, 1999 – 16 с. – (Нормативний документ). 13. Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 06.04.2001 №11: НД ТЗІ 2.3-002-2001 [чинний від 2001-04-10]. – К.: ДСТСЗІ СБ України, 2001 – 11 с. – (Нормативний документ). 14. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: НД ТЗІ 3.7-003-05. – [Чинний від 2005-11-08]. – К.: ДСТСЗІ СБ України, 2005. – 16 с. – (Нормативний документ системи технічного захисту інформації). 15. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги: ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. – [Чинний від 2010-01-01. – К.: Національний банк України, 2010. – 49 с. – (Галузевий стандарт України). 16. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 – [Чинний від 2010-01-01. – К.: Національний банк України, 2010. – 163 с. – (Галузевий стандарт України).
--	---

Висновок

Запропонована інформаційна модель захисту даних в технологіях зв'язку дозволяє забезпечити цілісну безпеку на рівні системи “об’єкт – загроза – захист” для передавально-приймального тракту “система – канал зв'язку – система”, що є методологічною основою для застосування уніфікованих методів і засобів захисту інформації згідно діючих стандартів у сфері інформаційно-комунікаційних технологій.

Список літератури

1. Закон України “Про Національну програму інформатизації” від 4 лютого 1998 року №74/98-ВР. Остання редакція від 02.12.2012. – [Електронний ресурс]. – Режим доступу: <http://zakon4.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80>.
2. Концепція технічного захисту інформації в Україні. Постанова Кабінету Міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” від 08.10.1997 № 1126. Остання редакція від 13.10.2011. – [Електронний ресурс]. – Режим доступу: <http://zakon4.rada.gov.ua/laws/show/1126-97-%D0%BF,415>.
3. Щербаков, В. Б. Защита беспроводных телекоммуникационных систем: учеб. пособие / В. Б. Щербаков, А. В. Гармонов, С. А. Ермаков и др. – Воронеж: ФГБОУ ВПО “Воронежский государственный технический университет”, 2013. – 127 с.
4. Рибачек, Н. І. Аналіз захищеності інформаційної системи / Н. І. Рибачек // К.: Національний технічний університет України “Київський політехнічний інститут”: Прикладна математика та комп’ютинг, 2010. – С. 122-125.

5. Kargl, F. Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges / F. Kargl, P. Papadimitratos, L. Buttyan and other // IEEE Communications Magazine. – November, 2008. – P. 110-118.
6. Дудикевич, В. Б. Захист засобів і каналів телефонного зв'язку: Навчальний посібник / В. Б. Дудикевич, В. В. Хома, Л. Т. Пархуць. – Л.: Видавництво Львівської політехніки, 2012. – 210 с.
7. Попов, В. И. Основы сотовой связи стандарта GSM / В. И. Попов. – М.: Эко-Трендз, 2005. – 296 с.
8. GSM Overview. Telecomspace. – [Електронний ресурс]. – Режим доступу: <http://www.telecomspace.com/gsm.html>.
9. Дудикевич, В. Б. Концептуальні моделі захисту інформації для технологій стаціонарного, стільникового, супутникового зв'язку / В. Б. Дудикевич, Ю. Р. Гарасим, Г. В. Микитин // Вісник Національного університету "Львівська політехніка": Автоматика, вимірювання та керування, 2010. – № 665. – С. 18-26.
10. Вайнгартнер, М. Защита голосовых соединений VoIP от прослушивания / М. Вайнгартнер // Журнал сетевых решений/LAN, 2003. – № 12. – [Электронный ресурс]. – Режим доступа: <http://www.osp.ru/lan/2003/12/138398>.
11. Челнокова, О. ADSL-маршрутизаторы с поддержкой VPN / О. Челнокова // Information Security / Информационная безопасность, 2008. – №2. – С. 32-33.
12. Ramachandran, V. BackTrack 5 Wireless Penetration Testing Beginner's Guide / V. Ramachandran. – Birmingham: Packt Publishing Ltd., September 2011. – 207 p.
13. Владимиров, А. А. Wi-фу: "боевые" приемы взлома и защиты беспроводных сетей. Серия "Защита и администрирование" / А. А. Владимиров, К. В. Гавриленко, А. А. Михайловский. – М.: NT Press, 2005. – 463 с.
14. Гордейчик, С. В. Безопасность беспроводных сетей / С. В. Гордейчик, В. В. Дубровин. – М.: Горячая линия - Телеком, 2008. – 288 с.

ИНФОРМАЦИОННАЯ МОДЕЛЬ БЕЗОПАСНОСТИ ТЕХНОЛОГИЙ СВЯЗИ

В.Б. Дудикевич¹, В.А. Хорошко², Г.В. Микитин¹, Р.І. Банах¹, А.І. Ребець¹

¹ Национальный авиационный университет,
пр. Космонавта Комарова, 1, Киев, 03058, Украина;

² Национальный университет «Львовская политехника»,
ул. С. Бандеры, 12, Львов 13, 79013, Украина, e-mail: professor_va@ukr.net

Предложена информационная модель безопасности данных в технологиях связи GSM, PSTN, VoIP, ADSL, Wi-Fi на уровне системы "объект - угроза - защита".

Ключевые слова: объект защиты, угроза информационной безопасности, технология защиты информации

INFORMATION SECURITY MODEL FOR COMMUNICATION TECHNOLOGIES

V.B. Dudikevich¹, V.O. Khoroshko², G.V. Mikitin¹, R.I. Banach¹, A.I. Rebets¹

¹ National University «Lviv Polytechnika»,
12 S.Bandera str., Lviv -13 , 79013, Ukraine

² National Aviation University,
1, prosp. Kosmonavta Komarova, Kiev, 03058, Ukraine; e-mail: professor_va@ukr.net

Information model for data security in GSM, PSTN, VoIP, ADSL, and Wi-Fi communication technologies at the level of "asset-threat-protection" system was proposed.

Keywords: asset to be protected, information security threat, information security technology.

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ СЦЕНАРИЕВ ПОВЕДЕНИЯ ВРЕДОНОСНЫХ ПРОГРАММ

В.М. Рувинская, А.В. Молдавская

Одесский национальный политехнический университет
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: amme4od@mail.ru

Статья посвящена проблеме автоматизированного формирования сценариев, описывающих поведение вредоносных программ. Приведены пути её поэтапного решения с помощью методов машинного обучения, обоснован выбор конкретных методов. Предложено представление сценариев в виде байесовских сетей. Применимость этого решения продемонстрирована на примере. Также описаны требования к обучающей выборке, выполнение которых на этапе сбора информации позволит увеличить точность работы методов машинного обучения. Проведены эксперименты, демонстрирующие повышение качества результата при повышении качества выборки.

Ключевые слова: вирусология, антивирус, сценарии, машинное обучение, ядерные функции, байесовские сети, структурное обучение.

Введение

Воздействие вредоносных программ на сегодняшний день является одной из основных угроз для компьютерных систем. Появление и распространение новых угроз происходит крайне быстро [1]. Вследствие этого быстрое обнаружение и идентификация новых вредоносных программ является основной задачей разработчиков антивирусного программного обеспечения. Быстрое и эффективное решение этой задачи с использованием исключительно статических методов, таких как ручной или автоматизированный сигнатурный анализ, сегодня невозможно по причине активного использования авторами вирусов техник, затрудняющих этот анализ (обфускация, полиморфизм, шифрование кода и т.д.). Однако одновременно с этим, поведение многих новых вредоносных программ остаётся типичным: отправка данных пользователя на сторонние адреса, генерация трафика, саморассылка и самокопирование [2]. В связи с этим растёт интерес к динамическим методам анализа, в частности, к методам поведенческого анализа вредоносных программ. Использование их совместно со статическими позволяет более полно и глубоко исследовать образцы угроз. Благодаря этому разработчики антивирусного программного обеспечения могут своевременно обнаруживать новые угрозы и вносить соответствующие изменения в антивирусные базы и каталоги вредоносных программ, предотвращая дальнейшее распространение этих новых угроз.

Работа посвящена вопросам автоматизированного формирования сценариев поведения вредоносных программ на основе обучения по примерам. Применение таких сценариев для обнаружения угроз было впервые предложено в [3]. Там же приведены примеры сценариев и предложен аппарат для их описания на основе регулярных выражений. Согласно [3], сценарий представляет собой модель представления знаний, описывающую обобщенное поведение как последовательность действий с учетом

альтернатив, циклов, а также иерархий с использованием регулярных выражений. Задание сценариев поведения вредоносных программ вручную – очень трудоёмкая задача. Поэтому *целью* нашего исследования является выбор методов машинного обучения, которые подходили бы для формирования описаний поведения вредоносных программ по примерам. Для этого следует решить такие *задачи*:

- изучить и проанализировать существующие методы машинного обучения, выбрать наиболее подходящие;
- описать требования к входным данным, выдвигаемые этими методами, в контексте наблюдения вредоносных программ;
- опробовать выбранные методы, оценить результат.

Обзор методов машинного обучения, подходящих для формирования сценариев

Задачу формирования сценария с помощью машинного обучения можно условно разделить на два этапа:

- получение списка событий сценария;
- получение связей между событиями.

Метод получения списка событий должен позволять обобщать действия различных вредоносных программ, носящие сходный характер. Очевидно, что перед нами, по сути, стоит задача классификации либо кластеризации. То есть методом получения списка событий может стать любой метод классификации большого количества данных. Однако нужно учитывать, что мы будем иметь дело с достаточно большим объёмом данных, которые также могут быть зашумленными вследствие наличия не совсем типичных вредоносных программ. Для этого придётся применять достаточно новые и развитые методы, а именно методы машинного обучения на ядерных функциях, адаптированные для классификации именно по большим объёмам прецедентов (так называемые ядерные методы) [4]. Они специально предназначены для классификации сильно перемешанных данных и хорошо справляются с зашумленными данными.

Ядерные методы обучения

Методы обучения на ядрах, также известные как ядерные машины (kernel machines), применяются в решении задач классификации и кластеризации. Идея методов состоит в том, чтобы представить пространство классифицируемых данных X , для которых не существует линейного разделителя, в пространстве более высокой мерности Y , где такой разделитель можно будет построить. Для осуществления этого необходимо вычислить для каждого вектора данных функцию нелинейного отображения $\Phi: x \rightarrow y$, где x – элемент пространства исходных данных X (более низкой размерности), а y – его проекция на пространство Y (более высокой размерности). Сложность такого вычисления возрастает пропорционально увеличению мерности пространства. Кроме того, мерность пространства Y может быть достаточно велика, и в таком случае $\Phi(x)$ вычислить невозможно. Решить данную проблему можно с помощью так называемого ядерного трюка. Для вычисления Φ используется скалярное произведение двух векторов, для которого требуется учитывать мерность пространств. Но возможно также заменить его специальной ядерной функцией $K(x, y)$, которая обладает свойствами скалярного произведения. В результате сама функция $\Phi(x)$ и, соответственно, мерность пространства перестают играть роль в вычислениях: теперь достаточно вычислить $K(x, y)$. То есть, использование ядерных функций позволяет использовать в пространстве Y те же алгоритмы, что для пространства X

без необходимости учитывать мерность Y . Алгоритмы, использующие этот приём, а вместе с ним и функцию $\Phi(x)$, и называют ядерными.

Для построения ядерной функции $\Phi(x)$ в общем виде достаточно следовать теореме Мерсера, приведенной в [5], которая определяет необходимые свойства функции. Там же приведены правила порождения функции. Также новые функции получают, осуществляя линейные комбинации и композиции существующих. При этом каждая конкретная функция оптимально подходит только для определённого ряда задач. Это связано с разнотипностью разброса данных в исходном пространстве в различных задачах, что нужно учитывать при переносе данных в пространство более высокой мерности.

После выбора ядра требуется решить задачу подбора числовых параметров ядерной функции. Существуют методы автоматического подбора параметров. Примерами наиболее точных являются довольно затратный метод поиска по сетке (grid search) и симплекс-метод Нелдера-Мида.

Важно различать ядерные функции и методы классификации или кластеризации с их использованием (ядерные машины): в один и тот же метод может быть внедрена произвольная ядерная функция. Достаточно, чтобы к этим методам был применим ядерный трюк.

Наиболее типовым и широко применяемым примером ядерных машин, используемых для классификации, являются машины опорных векторов (supporting vector machines, SVM). Метод опорных векторов осуществляет классификацию через отделение классов друг от друга гиперплоскостями, или линейными разделителями. По обеим сторонам линейного разделителя, или разделяющей гиперплоскости, строится ещё две гиперплоскости таким образом, чтобы полученные в результате классы находились вне отведённой ими области, или зазора. Качество классификации зависит от ширины образовавшегося между классами зазора. Примером метода кластеризации служит ядерный вариант алгоритма k-means. Метод k-means, или метод k -средних, находит кластеры, обнаруживая наиболее подходящие их центры, для чего нужно заранее знать количество кластеров. Ядерные функции позволяют применять эти методы в случаях с трудноразделимыми сильно перемешанными данными [6]. Их параметры настраивают таким образом, чтобы оптимизировать точность и гибкость работы метода. Например, константа c в методе SVM влияет на ширину зазора.

Методы структурного обучения. Применение байесовских сетей для описания сценариев

Получив список событий, следует определить связи между ними, чтобы получить сценарии. Обобщённое описание формата сценария приведено в [3]. Уточним, что каждое событие в этом формате называется целью либо подцелью вредоносной программы. Очевидно, следует построить сеть, связи в которой способны соответствовать необходимым регулярным выражениям. Кроме того, связи должны быть направленными, чтобы отражать причинно-следственные связи между событиями. Наконец, такая сеть должна быть вероятностной, чтобы обеспечить гибкость в принятии решений, которая наиболее важна в обнаружении новых модификаций известных угроз. Из всех применяемых сегодня вероятностных направленных графов, с описаниями некоторых из которых можно ознакомиться в [7], для нас наиболее подходящими являются байесовские сети. Это обусловлено тем, что байесовская вероятность является более гибкой по сравнению с частотной. Она способна обновляться по мере получения новой информации. Как частотная, так и байесовская вероятности оперируют с данными статистики. Однако частотная вероятность использует её лишь как описание параметров, а байесовская — для получения

вероятности того, что определённые параметры (выражаемые случайными переменными) достигнут определённого целевого состояния, причём при условии достижения другими связанными с ними параметрами определённых состояний. Итак, байесовская вероятность выражает причинно-следственные связи, демонстрируя каким образом (с какой вероятностью и при каких своих значениях) причины влияют на следствия [8]. Благодаря этому, её можно успешно использовать в задачах принятия решений (к каковым относится и наша задача). Что касается использования регулярных выражений в сценариях, предлагаемого в [3], то оно окажется заменено отношениями условной вероятности и условной независимости, как будет показано ниже. Условная вероятность – это вероятность выполнения одного события, если было выполнено другое. Условная независимость – это отношение между тремя переменными, в котором одна переменная передаёт информацию о зависимости между двумя другими [9].

Процесс построения байесовской сети с помощью некоторого алгоритма называется структурным обучением. По своему основанию и принципу работы алгоритмы обучения структуре делятся на классы, представленные ниже.

1. Основанные на ограничениях. Основной идеей алгоритмов, использующий данный метод, является проведение анализа условной независимости. В результате определяется, какие узлы связаны, а какие – нет. После этого строится «скелет» сети, то есть определяется структура графа без направлений. На последнем этапе определяются направления дуг. Возможная ошибка алгоритмов этого класса: на выходе могут быть получены неориентированные рёбра вследствие невозможности принятия однозначного решения.

Рассмотрим простейший алгоритм этой категории – алгоритм Петера-Кларка (PC) [10]. Он принимает за основу «наихудший» случай, в котором все переменные связаны со всеми (а потому структура образуется наиболее сложная из возможных). Далее ведётся поиск условно независимых друг от друга переменных, то есть таких, которые связаны между собой другими переменными. Раз связь между ними обеспечена промежуточными узлами, то непосредственная связь должна быть удалена. Благодаря этому будет видно, как первая переменная влияет на вторую с учётом влияния промежуточных переменных. Если же оставить непосредственную связь, эта информация окажется потеряна.

Другими, более сложными, но и более перспективными алгоритмами являются, например, американский SLA (Simple Learning Algorithm) [11] и корейский SCD (Sequential Causal Discover) [12]. Оба они используют свойства и особенности байесовских сети как вероятностного направленного графа.

2. Метрические. Основаны на мере качества, т.е. достоверности сети. Такие алгоритмы находят наиболее вероятную структуру сети, причём вероятность вычисляется на основе специальной метрической функции (иначе называемой метрикой либо функционалом качества). Возможная ошибка алгоритмов данного класса: установление ошибочных связей.

Одной из наиболее широко используемых сегодня метрик является K2 [14, 15]. Она образована из формулы Байеса, в которую в качестве аргументов подставлены исходная база и искомая структура. Суть работы алгоритма на основе данной метрики заключается в следующем. В ходе работы алгоритма для каждой случайной переменной x_i ($i \in [1, n]$, где n – количество переменных) производится оценка всех возможных её родителей и их комбинаций с помощью метрической функции. Наибольшее вычисленное значение функции соответствует наиболее вероятному набору родителей. Для вычисления используется подсчёт в обучающей выборке количества комбинаций всех возможных значений родителей и самой переменной x_i . То есть, вероятность того, что переменная x_j ($j \in [1, n]$, где n – количество

переменных) является родителем x_i , зависит от того, сколько раз встречается одна и та же комбинация их возможных значений в базе. Это объясняется тем, что часто встречающиеся комбинации выражают собой некоторую закономерность, существующую между случайными переменными. Эта закономерность и является искомой связью, то есть частью искомой структуры.

Существуют также метрики, основанные на теории информации. По своему принципу работы они достаточно сильно отличаются от класса байесовых. В них существуют механизмы для поиска наиболее компактной структуры сети, однако вместе с этим данные алгоритмы могут страдать от переобучения, или оверфиттинга (ошибочного обнаружения закономерностей в обучающей выборке, которых в реальности не существует) либо излишней вычислительной сложности. Известные примеры метрик на основе теории информации – информационный критерий Акаике (AIC) и родственный ему информационный критерий Байеса (BIC).

Эксперименты показали [14], что метрики байесовой группы на больших выборках работают успешнее информационных, но проигрывают им на небольших. Алгоритмы же на основе ограничений могут строить сеть не полностью, сталкиваясь с неопределённостями [10], чего с метрическими алгоритмами не происходит. Исходя из сказанного, в нашей задаче предпочтительнее использование метрик на основе теоремы Байеса.

Структурное обучение – ресурсоёмкая задача, поскольку зачастую не удаётся избежать использования так называемого «жадного поиска» нужного графа в пространстве графов либо других вычислительно сложных элементов алгоритма. Сократить объёмы вычислений позволяет предварительное упорядочивание переменных, что указано в спецификациях ряда алгоритмов [11–13]. В результате, поиск родителей и комбинаций родителей для каждой переменной ведётся только среди предваряющих её переменных. Во многих задачах такое требование к исходным данным является неудобным ограничением, требующим вмешательства эксперта, и от него стремятся избавиться. Однако в задаче построения сценария оно превращается в преимущество: поскольку мы наблюдаем следующие друг за другом события, то переменные окажутся естественным образом упорядочены ещё на этапе построения списка переменных (то есть на этапе классификации).

Требования к качеству обучающей выборки

Успешность построения сети напрямую зависит от качества обучающей выборки, а именно от репрезентативности и зашумленности входных данных. В том случае, когда от зашумленности не удаётся избавиться, можно снизить её влияние, дополнив выборку большим количеством лишённых шума данных. Более сложной задачей является обеспечение достаточной репрезентативности. В общем виде оно достигается тем, что в процессе эксперимента следует добиваться того, чтобы каждая рассматриваемая случайная переменная принимала все свои возможные значения, после чего отследить, как это отразилось на состояниях всех прочих переменных. То есть, следует обеспечить разнообразие результатов. Благодаря тому, что в наблюдаемом поведении или модели существуют скрытые связи (которые и должен выявить алгоритм структурного обучения), это разнообразие позволит прояснить закономерности. Обучающая выборка должна демонстрировать функции вредоносной программы так, чтобы передавать их специфичность и взаимосвязь друг с другом. То есть, при проведении экспериментов следует охватить как можно больше вариантов поведения каждой вредоносной программы. Для этого недостаточно только наблюдения за поведением вредоносной программы в нормальных условиях, где она будет успешно выполнена от начала до конца. Необходимо также обеспечить условия,

в которых активность любой функции вредоносной программы можно прервать, не затрагивая прочих её функций. Тогда, если некоторые другие функции зависят от прерванной, они также не выполняются, что и будет зафиксировано в результатах эксперимента. Следовательно, будет обнаружена условная независимость между прерванной функцией и всеми прочими.

Опробование метода построения структуры сценария на основе байесовской сети

Рассмотрим на тестовом примере, как качество входных данных влияет на точность построения сети. Возьмём выборку по поведению некоторого количества почтовых червей из энциклопедии SecureList от Лаборатории Касперского [15]. Она приведена в таблице 1. В данной выборке значение 1 соответствует выполнению события, значение 0 – невыполнению.

Составленный Лабораторией Касперского [16] на основе жизненного цикла червя сценарий поведения приведен на рис.1.

Таблица 1.

Выборка с данными по поведению типовых почтовых червей

Наименование	Создани е копии на диске	Изменен ие реестра	Сканирова ние адресной книги	Сканиро вание файлов	Саморас сылка
Email-Worm.VBS.Challenge	1	1	1	0	1
Email-Worm.Win32.Silver	1	1	1	1	1
Email-Worm.VBS.KakWorm	1	1	1	0	1
Email-Worm.Win32.Mintal.003	1	1	1	0	1
Email-Worm.Win32.Sober.a	1	1	0	1	1
Email-Worm.JS.Nevezed	1	0	1	0	1
Email-Worm.Win32.Dumaru.b	1	1	0	1	1
Email-Worm.Win32.Gismor	1	1	1	0	1
Email-Worm.JS.Sigbug	1	1	1	0	1
Email-Worm.Win32.Hermes.a	0	0	1	0	1
Email-Worm.Win32.Pepex.a	1	1	0	1	1
Email-Worm.Win32.SysClock	1	1	1	1	1
Email-Worm.Win32.Scorpion	1	1	1	0	1

В выборке зафиксировано нормальное поведение 13 наименований червей в условиях, где они не встретили никаких препятствий для своей работы. Попробуем построить байесовскую сеть на основе таких данных с помощью алгоритма структурного обучения. Воспользуемся для этого метрическим алгоритмом K2, так как его результаты работы легче для понимания и демонстрации, чем результаты работы метрических алгоритмов на основе теории информации и алгоритмов на ограничениях. Алгоритм на основе теоремы Байеса K2 вычисляет вероятности всех возможных вариантов структуры сети, что может пригодиться для оценки того, где и насколько ошибся алгоритм в процессе обучения и соответствующим образом скорректировать структуру. Результат работы алгоритма (наиболее вероятная для данных из табл. 1 структура графа) приведен на рис. 2.

Из этого результата следует, что для рассылки копий на другие электронные адреса с зараженного компьютера программе-червю достаточно создать свою копию на жёстком диске этого компьютера. От сканирования же адресной книги или файлов на

диске (откуда на самом деле червь и извлекает адреса для рассылки) это действие якобы не зависит. Очевидно, результат в этом месте содержит ошибку.

Дополним теперь исходную выборку таким образом, чтобы она содержала не только данные о том, как ведёт себя червь в норме, но и о том, что будет происходить с его действиями при невыполнении одного из них. Эти дополнительные данные представлены в таблице 2.

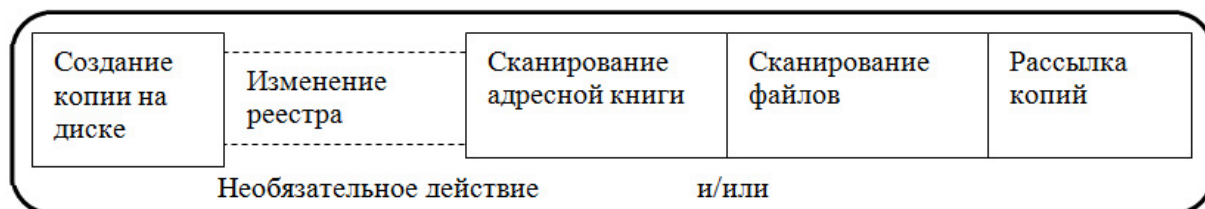


Рис. 1. Типичный сценарий поведения почтового червя

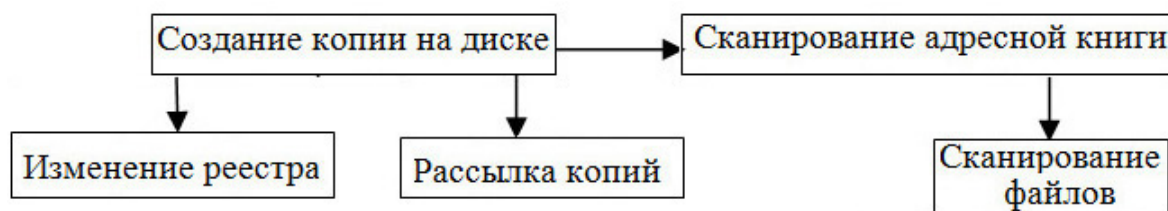


Рис. 2. Результат структурного обучения сети на основе первого варианта выборки

Таблица 2.

Дополнительные данные о поведении червя с условием прерывания некоторых событий

Наименование	Создание копии на диске	Изменение реестра	Сканирование адресной книги	Сканирование файлов	Саморассылка
Email-Worm.VBS.Challenge	1	1	1	0	1
Email-Worm.VBS.Challenge	1	0	0	0	0
Email-Worm.VBS.Challenge	1	1	0	0	0

Поясним эти данные. В первой строке мы для наглядности оставили нормальное поведение червя. Во второй предположили, что изменение реестра (а именно, запись червя в автозапуск) не произошло. Поскольку работа червя построена на активации в виде программы автозапуска, невыполнение данного события означает невозможность выполнения всех остальных функций червя. Поэтому все соответствующие события принимают значение 0. В третьей строке предполагаем, что не произошло сканирования адресной книги. Учитывая, что сканирование файлов данный червь не способен выполнить, саморассылка оказывается невозможной и тоже приобретает значение 0.

Таким образом, выборка приобрела больше репрезентативности, то есть более полно описывает предметную область. Результат работы алгоритма K2 с новой выборкой приведен на рис. 3.

Поясним этот результат. Тот факт, что из изменения реестра не следует ни один из следующих узлов, говорит о том, что изменение реестра является необязательным событием в сценарии, что соответствует экспертной версии. Сканирование файлов действительно следует из сканирования адресной книги: если червь не сканировал адресную книгу, вероятность того, что он будет сканировать файлы, повышается, так как из файлов тоже можно извлекать адреса электронной почты. Рассылка копий следует как из сканирования адресной книги, так и из сканирования файлов по той же причине: адреса можно получить из обоих источников. Сходящаяся связь аналогична отношению «и/или». Таким образом, сеть построена верно и полностью соответствует сценарию.

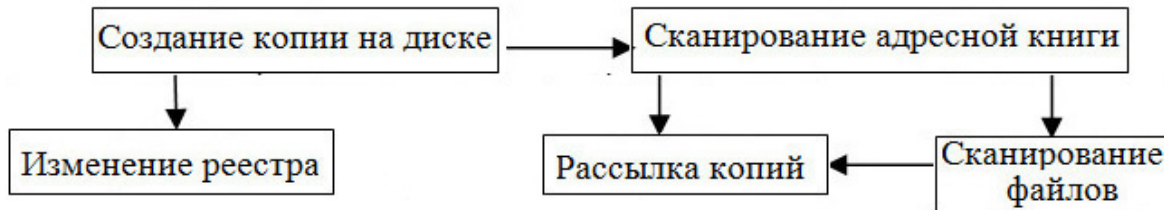


Рис. 3. Результат структурного обучения сети на основе второго варианта выборки

Выводы

Сделан вывод, что использование механизмов машинного обучения для формирования сценариев возможно. Преимущества этого подхода по сравнению с ручным составлением сценариев заключаются в минимизации нагрузки на эксперта при составлении базы знаний для экспертной системы, использующей сценарии. Были описаны особенности работы с ядерными машинами, применяемыми в классификации и кластеризации. Сделан вывод, что они подходят для формирования обобщённых классов поведения вредоносных программ. Рассмотрена возможность построения сценариев с помощью методов машинного обучения, применяемых в обучении байесовских сетей. Представление в виде байесовских сетей позволяет выразить причинно-следственные связи между событиями, а также ветвление, которое часто встречается в сценариях. Было продемонстрировано, как сетевая структура отображает обязательные и необязательные подцели, регулярное выражение «и/или». Кроме того, были разработаны требования к обучающей выборке, после чего было экспериментально подтверждено их влияние на точность результата при выполнении структурного обучения.

В последующих исследованиях может быть рассмотрена возможность представления циклов в сценариях, построенных на ациклических байесовских сетях. Дальнейшим направлением работы станет также углубление описания сценария как структуры данных.

Список литературы

1. Mansfield-Devine, S. Significant rise in cybercrime against public sector organisations. / Steve Mansfield-Devine. – Computer Fraud & Security, Issue 1. – 2012. – p.1-3.
2. Honig, A. Practical Malware Analysis. / A. Honig. – No Starch Press, 2012. – 800 p.
3. Рувинская, В. М. Эвристические методы детектирования вредоносных программ на основе сценариев / В. М. Рувинская, Е. Л. Беркович, А. А. Лотоцкий // Искусственный интеллект. – 2008. – № 3. – С. 197-207.

4. Gammerman, A. Hedging Predictions in Machine Learning. / A. Gammerman, V.Vovk // Comput. J. 50, 2. – 2007. – p. 51-163.
5. Wang R. Introduction to Orthogonal Transforms. / Ruye Wang //Cambridge University Press. – 2012. – 590 p.
6. Grigorios F. Tzortzis. The global kernel k-means algorithm for clustering in feature space./ G. F. Tzortzis , A. C. Likas // IEEE Transactions on Neural Networks, v.20 – 2009. – n.7. – p.1181-1194.
7. Толпин, Д.А. Вероятностные сети для описания знаний /Д.А. Толпин // Информационные процессы. – М.: Русинвест, 2007. – т. 7, № 1. – с.93-103.
8. Ullman, D.G. Making Robust Decisions. / D.G. Ullman // Trafford Publishing. – 2006. – 348 p.
9. Тулупьев, А. Л. Байесовские сети: логико-вероятностный подход. / А.Л. Тулупьев, С.И. Николенко, А.В. Сироткин. – СПб. : Наука, 2006. – 608 с.
10. Spirtes, P. Causation, Prediction, and Search. / P. Spirtes, C. Glymour & R. Scheines // MIT Press, Adaptive Computation and Machine Learning, second edition. – 2006. – 549 p.
11. Cheng, J. Learning Bayesian Networks from Data: An Information-Theory Based Approach. / J. Cheng, R. Greiner, J. Kelly. //University of Ulster. – 2001. – 74 p.
12. Lee, S. A New Polynomial Time Algorithm for Bayesian Network Structure Learning. / S. Lee, J. Yang, S. Park. // Berlin, ADMA. – 2006. – p.501-508.
13. Cooper, F.G. A bayesian method for the induction of probabilistic networks from data. / F. G. Cooper, E. Herkovits // Stanford University School of Medicine, Stanford – 1993. – 39 p.
14. Carvalho, A.M. Scoring functions for learning Bayesian networks. - Tec. Rep. / Alexandra M. Carvalho // INESC-ID 54/2009. – 2009. – 48p.
15. SecureList - Новые описания детектируемых объектов. [Электронный ресурс] // Режим доступа: <http://www.securelist.com/ru/descriptions>
16. Вирусы и средства борьбы с ними. Учебный курс. [Электронный ресурс] // Режим доступа: <http://www.csid.omsu.omskreg.ru/docs/docs/viruses.pdf>

ЗАСТОСУВАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ФОРМУВАННЯ СЦЕНАРІЇВ ПОВЕДІНКИ ЗЛОВМИСНИХ ПРОГРАМНИХ ЗАСОБІВ

О.В. Молдавська, В.М. Рувінська

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: amme4od@mail.ru

Стаття присвячена проблемі автоматизованого формування сценаріїв, що описують поведінку зловмисних програм. Приведено шляхи її поетапного розв'язання за допомогою сценаріїв, обґрунтовано вибір конкретних методів. Запропоновано представлення сценаріїв за допомогою баєсівських мереж, продемонстровано результати експериментів на вибірках даних різного рівня якості.

Ключові слова: зловмисне програмне забезпечення, сценарії, машинне навчання, ядерні функції, баєсівські мережі, структурне навчання

USING MACHINE LEARNING METHODS TO FORM THE SCENARIOS OF BEHAVIOR OF MALICIOUS SOFTWARE

A.V. Moldavskaya, V.M. Ruvinskaya

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: amme4od@mail.ru

The paper is devoted to the problem of computer-aided forming of scenarios, with the latter describing the behavior of malicious software. The means of step by step problem solution using machine learning methods were discussed, and the choice of specific methods was substantiated. Presenting the possible scenarios in the form of Bayesian networks was proposed. Applicability of this approach was exemplified. Moreover, there were described the requirements to learning sample, which, if met at the data acquisition stage, would increase the accuracy of operation of machine learning methods. The experiments were conducted to demonstrate the improvement of the result quality with improvement of sample quality.

Keywords: virusology, antivirus, scenario, machine learning, nuclear functions, Bayesian networks, structural learning.

ГРАФОВА МОДЕЛЬ СТАНІВ КОРИСТУВАЧА СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ

С.В. Ленков¹, О.О. Гайша², Є.С. Ленков³

¹ Військовий інститут Київського національного університету імені Тараса Шевченка,
вул. Ломоносова, 81, Київ, 03680, Україна; e-mail: lenkov_s@ukr.net

² Національний університет кораблебудування імені адмірала Макарова,
просп. Героїв Сталінграду, 9, Миколаїв, 54025, Україна

³ Національний авіаційний університет,
просп. Космонавта Комарова, 1, Київ, 03058, Україна

Обґрунтована необхідність використання моделі станів користувача в системах дистанційного навчання (СДН). Для створення моделі весь навчальний матеріал СДН розбивають на множини елементарних невідимих відомостей певного типу: означень, пояснень, формул, схем, теорем, описів, і т.д. Для даного користувача формується набір відомостей, які йому необхідно засвоїти. Далі у якості стану користувача по кожному предмету розглядають наступну трійку: множина всіх вивчених і перевірених відомостей, множина всіх вивчених і ще не перевірених відомостей, множина всіх отриманих оцінок за контрольні роботи. Ще система працює з множинами елементарних відомостей, що перевіряються певними стандартними контрольними роботами, а також з набором стандартних дій користувача, що дозволяють йому переходити з одного стану в інший. На основі цих величин формується графова модель станів користувача СДН, що відповідає процесу його навчання.

Ключові слова: граф, множина, електронне навчання, дистанційна освіта

Вступ

В процесі навчання особа (в подальшому використовуватимемо термін «студент» безвідносно до освітньо-кваліфікаційного рівня, який здобуває дана особа) набуває певного обсягу знань та умінь, що більше чи менше відповідає навчальним програмам і планам (залежно від ступеня засвоєння матеріалу кожним окремим студентом). При звичайному процесі навчання поруч із студентом постійно перебувають професійні викладачі, що коригують цей процес відповідно до поточного моніторингу рівня засвоєння знань. При дистанційному навчанні контроль з боку викладача зведений практично до нуля: більшість матеріалу студенти вивчають самостійно і також самостійно мають проходити самостійний, поточний, проміжний та (часто) вихідний контроль в автоматизованому комп'ютерному режимі.

Отже, при такому підході у програмно-технічному комплексі забезпечення дистанційної освіти (ДО) мають бути присутніми певні засоби (забігаючи наперед скажемо, що це має бути інформаційна система - ІС), що в деякій мірі могла б замінити викладача, а саме – здійснювати загальний аналіз поточної ситуації в навчанні по групі, по окремому студенту, окремій дисципліні, окремій дисципліні у окремого студента, окремій темі, окремій темі у окремого студента. При необхідності ця ІС має здійснювати коригування процесу навчання: рекомендувати або примушувати до повторного вивчення слабо засвоєних розділів залежно від результатів проміжного контролю; переривати процес вивчення теми, якщо при поточному контролі вияснилося, що якась із попередніх тем, на якій базується дана, не засвоєна належним

чином (наприклад, вивчалася давно і студент її забув) і її слід повторити. Часто матеріал курсу ВНЗ базується на інформації, що вивчається у старших класах і міг бути позабутий студентами, отже в ІС повинна існувати можливість надання цієї інформації для повторення. Також можлива ситуація – зосередження студента лише на одному (кількох) улюблених предметах у збиток більшості інших. ІС має постійно слідкувати за прогресом студента у різних предметах і при виявленні «перекосів» пропонувати йому ті предмети, за якими виявлено відставання.

Усі наведені приклади говорять про значну складність ІС, що керує процесом дистанційного навчання. Зведення такої системи не можливе без використання моделі процесу навчання окремого студента, що буде виконано в даній роботі. В цілому, з точки зору ВНЗ важливим є також процес навчання сукупності студентів (групи, напряму, спеціальності, курсу, факультету, тощо) і тому в подальшому необхідне створення ще і моделі процесу навчання заданого числа осіб.

Аналіз останніх досліджень і публікацій

Суттєвий внесок у дослідження адаптивних систем дистанційного навчання (СДН) зробив Федорук П.І. [1], в роботі якого зокрема розглядається використання графоавтоматної моделі у вигляді орієнтованого графу, вершини та ребра якого являють собою структурні автомати різних конструкцій. При підході [1] методика роботи з моделлю більше відповідає слідуванню певним алгоритмом, а не аналізу набору станів системи (чи користувача системи) і зв'язків між ними. Крім того, автор розглядає вивчення одного курсу (що складається із сукупності елементарних фактів – квантів), а не сукупності окремих курсів-дисциплін, що необхідно для побудови моделі процесу навчання у вищій школі. Розглядання сукупності курсів, що мають одночасно вивчатися студентом, вносить певні особливості у моделювання процесу його навчання.

Принципи роботи з графовими моделями станів різноманітних систем докладно описані в [2] та [3], але особливості роботи саме систем навчання, звичайно, не враховуються.

Таким чином, зважаючи на відсутність відповідної моделі, метою роботи є створення моделі процесу навчання окремого студента у вигляді графу станів.

Основна частина

Весь наявний в системі електронного навчання матеріал розіб'ємо на N частин, що відповідають окремим дисциплінам (в загальному випадку ці частини можуть перекриватися). Кожну таку n -ну частину (дисципліну) після докладного аналізу можна представити як множину U_n найменших нерозривних частин навчального матеріалу («атомів», «квантів» інформації) різних типів, таких як означення, формула, теорема, факт, опис експерименту, схема, відомості про певний об'єкт, і т.д. Типи таких інформаційних «атомів», допустимих для кожної дисципліни, можуть бути різними. Наприклад, для математики не може бути елементарної інформації типу «вірш», що є необхідним для літератури; для історії не потрібно типу «формула», і т.д. Для кожної n -ої дисципліни буде своя множина типів V_i , де $i = 1 \dots i_n$ — номер типу інформації, допустимого для n -ої дисципліни, а i_n — загальна кількість таких допустимих типів. Тоді всю множину U_n представляємо як об'єднання множини $U_n^{(1)}$ усіх відомостей типу V_1 із даної дисципліни, множини $U_n^{(2)}$ усіх відомостей типу V_2 із даної дисципліни, множини $U_n^{(3)}$ і т.д. до $U_n^{(i_n)}$:

$$U_n = U_n^{(1)} \cup U_n^{(2)} \cup \dots \cup U_n^{(in)}.$$

У будь-якій СДН для користувача, що вчиться за даною конкретною програмою (напрямом чи спеціальністю), можна виділити із всього простору наявної інформації набір множин U_n окремих дисциплін, об'єднати їх елементи, і в результаті отримаємо інформацію U , що слід засвоїти за семестр:

$$U = \bigcup_{n=1}^N U_n.$$

Перейдемо до станів користувача в СДН. Нехай уся їх сукупність утворює скінченну множину $\Omega = \{\omega_1, \dots, \omega_M\}$. Кожен елемент Ω відповідає якому-небудь конкретному стану користувача в СДН і являє собою підмножину ω_m , зміст якої розглянемо нижче. Перехід між станами здійснюється після завершення користувачем дії певного типу (можливо, ще і з деякою інерційністю) із множини усіх типів дій в СДН $A = \{\alpha_1, \alpha_2, \dots, \alpha_p\}$. Серед найбільш типових дій можна назвати:

- α_1 = «вивчення елементарної нерозривної частини навчального матеріалу», наприклад факту, формули, схеми, і т.д., тобто одного конкретного j -го елемента u_{nij} із якої-небудь множини $U_n^{(i)}$;

- α_2 = «вивчення певного розділу/модуля предмету»;
- α_3 = «вивчення певного предмету U_n »;
- α_4 = «проходження проміжного контролю»;
- α_5 = «проходження підсумкового контролю з дисципліни»;
- α_6 = «здача сесії U », і т.д.

Стани користувача ω_m можна розрізняти за трьома показниками:

- набором вивчених і перевірених шляхом контролю елементарних відомостей – множина W . Ця множина складається із підмножин W_{nq} , кожна з яких відповідає одному проведеному контрольному заходу (n — номер дисципліни, з якої дана контрольна; q — номер контрольної з даної n -ої дисципліни). W_{nq} містить елементарні відомості, засвоєння яких можна перевірити q -ою контрольною з дисципліни n ; потужність $|W_{nq}|$ дорівнює числу таких елементарних відомостей. Кількість елементів у W :

$$|W| = \sum_{n=1}^N \sum_{q=1}^{Q_n} |W_{nq}|,$$

де Q_n — кількість контрольних за n -ою дисципліною.

Множини W_{nq} можуть формуватися кожен раз оригінально (вручну) при проведенні контрольного заходу із окремих елементів u_{nij} множини U , або краще (розглядаємо в подальшому тільки такий варіант) — беруться із множини X усіх допустимих контрольних. Елементами такої множини є підмножини X_{nq} , що складаються із елементарних відомостей u_{nij} , засвоєння яких можна перевірити q -ою контрольною з дисципліни n .

▪ набором вивчених, але ще не перевірених шляхом контролю елементарних відомостей – множина W' . Відмітимо, що множина W' не обов'язково містить при даному стані користувача якісь конкретні X_{nq} , а вона лише містить набори u_{nij} , що необов'язково відповідають якій-небудь X_{nq} :

$$\exists j_1, j_2 : W' = \{u_{nij} \mid n=1 \dots N, i=1 \dots i_n, j=j_1 \dots j_2\}, X_{nq} \not\subset W' \forall n, q.$$

На початок контрольного заходу W_{nq} в ідеалі $X_{nq} \subset W'$, тобто користувач готовий до контрольної і знає усі факти, що в ній використовуються. Після проведення контрольного заходу і виставлення оцінки, W' оновлюється:

$$W' = W' \setminus X_{nq}.$$

▪ набором оцінок, отриманих за перевірені контрольні заходи, що вже містяться у W , це множина G . Для легшого співставлення конкретної контрольної W_{nq} та оцінки, отриманої по ній, зручно множину G організувати як і множину W : приймаємо, що G складається із n підмножин, в яких містяться оцінки по окремим дисциплінам. Кожному елементу W_{nq} із W відповідає один конкретний елемент G_{nq} із множини G , а точніше її підмножини G_n , тобто задана взаємно однозначна відповідність $W \Rightarrow G$. Так як елементи W є підмножинами, що включають усі перевірені на даному контрольному заході елементарні відомості, то за відповідним елементом множини G можна легко встановити, яку оцінку мав користувач за кожен конкретний елемент u_{nij} (точніше за контрольну роботу, яка була націлена на перевірку в тому числі u_{nij}).

Таким чином, зміст m -го стану користувача в СДН задається трійкою множин W, W', G :

$$\omega_m = \{W, W', G\}.$$

Як уже зазначалося вище, переходи між окремими станами ω_m можливі після завершення дії α_p . Деякі переходи здійснюються зі 100% імовірністю (мають неминучий характер, лише займають певний час), такі, як наприклад, визначені вище $\alpha_1, \alpha_2, \alpha_3$. Інші види переходів (наприклад, $\alpha_4, \alpha_5, \alpha_6$, визначені вище) навпаки мають певну імовірність успіху і невдачі, які можуть визначатися або безособово (на основі статистичної частоти успішної здачі даного контрольного заходу W_{nq} , предмету U_n або сесії U в цілому попередніми студентами) або відносно даного студента (враховуючи певним способом його попередню успішність). В цілому, визначення таких ймовірностей представляє собою достатньо складну задачу і потребує окремого дослідження.

Зважаючи на вищенаведене, процес навчання особи в СДН у першому наближенні може бути змодельований зваженим графом, вершини якого відповідають окремим ω_m , а переходи діляться на два типи (детерміновані та імовірнісні). Частина такого графу показана на рис. 1. На рисунку імовірності підписані тільки для переходів, що не є детермінованими. Дії α_p , що викликають зміну стану користувача СДН, підписані біля дуг, що зручно з точки зору використання місця на рисунку, але не зовсім точно, адже дія для цього графа є не характеристикою процесу зміни стану, а активатором цього процесу (відповідно, більш правильно було би сказати, що дії належать вершинам

графів і показують, яка саме дія користувача може змінити стан ω_m , в якому він знаходиться в поточний момент).

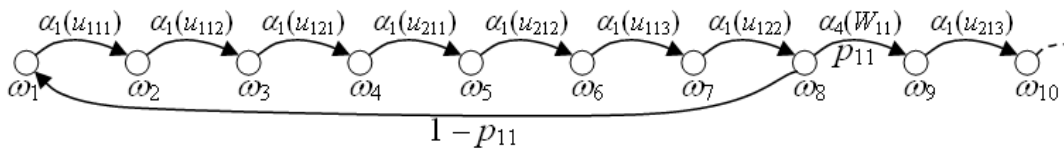


Рис. 1. Простий граф станів користувача в СДН

Процес навчання при такому графі виглядає наступним чином: користувач починає вчити дисципліну $n=1$ і вивчає (дія α_1) відомості u_{111} , u_{112} , u_{121} , а потім (наприклад, наступного дня) переключається на дисципліну $n=2$ і вивчає відомості u_{211} , u_{212} . Потім знову вертається до вивчення першої дисципліни – вчить відомості u_{113} , u_{122} і потрапляє до стану ω_8 , що характеризується переліченим набором $W' = \{u_{111}, u_{112}, u_{121}, u_{211}, u_{212}, u_{113}, u_{122}\}$ і двома порожніми множинами W і G :

$$\omega_8 = \{\emptyset, \{u_{111}, u_{112}, u_{121}, u_{211}, u_{212}, u_{113}, u_{122}\}, \emptyset\}.$$

Вихід із стану ω_8 ініціює дія типу α_4 – проходження контрольного заходу, а саме W_{11} – контрольної з дисципліни 1, по розділу 1. Якщо оцінка є успішною, то здійснюється перехід у стан ω_9 , імовірність чого складає p_{11} . При цьому до множини W усього вивченого і перевіреного матеріалу переноситься W_{11} , а з множини W' видаляються елементи, що входять до складу W_{11} . До множини G , а точніше до її підмножини G_1 вноситься отримана за контрольну W_{11} оцінка. Якщо ж контрольна виконана невдало, то необхідно повернутися до вивчення пройденого за дисципліною 1 матеріалу, тобто відбувається перехід у стан ω_1 . Якраз тут криється суттєвий недолік запропонованої форми графу станів: у лінійній послідовності станів $\omega_1 - \omega_8$ присутні як стани, що відрізняються вивченими відомостями по дисципліні 1, так і відомостями по іншій дисципліні 2, повторне вивчення яких не може бути визначене в результаті написання контрольної W_{11} .

Для більш адекватного описання процесу навчання розіб'ємо весь процес навчання на n підпроцесів і для кожного з них формуватимемо свій граф типу рис. 1. Тоді при повторному вивченні користувач має пройти лише через необхідний ряд станів, пов'язаних зі збільшенням відомостей саме по n -ій дисципліні, з якої була провалена контрольна. Щоб використовувати набір таких графів слід замість одного стану ω_m використовувати набір $\omega_m^{(1)}, \omega_m^{(2)}, \dots, \omega_m^{(N)}$, де верхній індекс відповідає номеру дисципліни. Кожна така підмножина $\omega_m^{(n)}$ відповідає стану користувача саме по n -ій дисципліні і являє собою трійку:

$$\omega_m^{(n)} = \{W^{(n)}, W'^{(n)}, G^{(n)}\},$$

де

$W^{(n)}$ — зберігає весь набір вивчених і перевірених елементарних відомостей u_{nij} з n -ої дисципліни;

$W'^{(n)}$ — містить набір вивчених, але ще не перевірених елементарних відомостей u'_{nij} з n -ої дисципліни;

$G^{(n)}$ — містить набір оцінок з контрольних робіт саме по n -ій дисципліні.

Повні множини усіх вивчених і перевірених відомостей W , усіх вивчених і не перевірених відомостей W' та усіх оцінок G формуються шляхом об'єднання відповідних множин за усіма дисциплінами:

$$W = \bigcup_{n=1}^N W^{(n)},$$

$$W' = \bigcup_{n=1}^N W'^{(n)},$$

$$G = \bigcup_{n=1}^N G^{(n)}.$$

Стани $\omega^{(n)}_m$ та відповідні переходи між ними повинні зображуватися на окремих графах, що характеризуватимуть навчання окремо за n -ою дисципліною (від цих часткових станів при необхідності завжди можна перейти до повного стану користувача в СДН). Переходи по цим графам відбуваються паралельно, тому умовно їх можна зобразити у вигляді графів, що лежать у паралельних площинах (рис. 2).

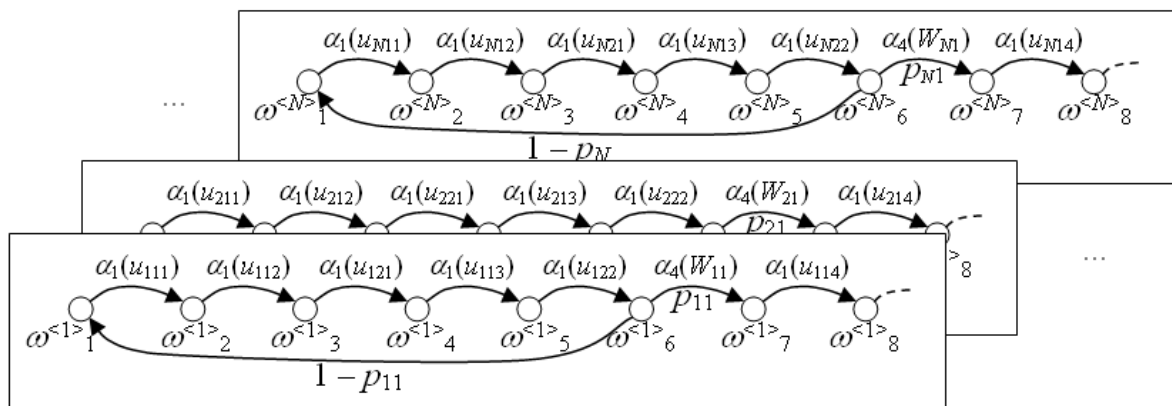


Рис. 2. Сукупність графів станів користувача в системі СДН (кожен граф відповідає одній навчальній дисципліні; структура усіх графів оригінальна)

Висновки

В роботі виконано моделювання процесу навчання одного окремого користувача СДН з використанням теорії множин та графів. Визначено основні елементи моделі та зв'язки між ними. Результати роботи можна використати при побудові моделі процесу навчання сукупності студентів (зокрема, навчальної групи), що планується в подальших дослідженнях.

Список літератури

1. Федорук, П.І. Адаптивна система дистанційного навчання та контролю знань на базі інтелектуальних Інтернет-технологій: автореф. дис... д-ра техн. наук: 05.13.06 / П.І. Федорук ; НАН України, Ін-т пробл. мат. машин і систем. — К., 2009. — 37 с.

2. Басакер, Р. Конечные графы и сети [Текст] : монография / Р. Басакер, Т. Саати ; ред. А.И. Тейман ; пер.: В.Н. Бурков, С.Е. Ловецкий, В.Б. Соколов. — М. : Наука, 1974. — 366 с.
3. Брегман, В.И. Графы в задачах управления производством [Текст] : произв.-практическое изд. / В.И. Брегман. — М. : Статистика, 1974. — 144 с.

ГРАФОВАЯ МОДЕЛЬ СОСТОЯНИЙ ПОЛЬЗОВАТЕЛЯ СИСТЕМЫ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ

С.В. Ленков¹, О.О. Гайша², Е.С. Ленков³

¹ Военный институт Киевского национального университета имени Тараса Шевченко, ул. Ломоносова, 81, Киев, 03680, Украина; e-mail: lenkov_s@ukr.net

² Национальный университет кораблестроения имени адмирала Макарова, просп. Героев Сталинграда, 9, Николаев, 54025, Украина

³ Национальный авиационный университет, просп. Космонавта Комарова, 1, Киев, 03680, Украина

Обоснована необходимость использования модели состояний пользователя в системах дистанционного обучения (СДО). Для создания модели весь учебный материал СДО разбивают на множества элементарных неделимых сведений определенного типа: определений, пояснений, формул, схем, теорем, описаний и т.д. Для данного пользователя формируется набор сведений, которые ему необходимо усвоить. Далее в качестве состояния пользователя по каждому предмету рассматривают следующую тройку: множество всех изученных и проверенных сведений, множество всех изученных и еще не проверенных сведений, множество всех полученных оценок за контрольные работы. Еще система работает с множествами элементарных сведений, которые проверяются определенными стандартными контрольными работами, а также с набором стандартных действий пользователя, которые позволяют ему переходить из одного состояния в другое. На основе этих сведений формируется графовая модель состояний пользователя в СДО, соответствующая процессу его обучения.

Ключевые слова: граф, множество, электронное обучение, дистанционное образование

GRAPH MODEL FOR THE STATES OF DISTANCE LEARNING SYSTEM USER

S.V. Lenkov¹, A.A. Gaisha², E.S. Lenkov³

¹ Military Institute, Taras Shevchenko National University of Kyiv, 81 Lomonosov str., Kyiv, 03680, Ukraine; e-mail: lenkov_s@ukr.net

² Admiral Makarov National University of Shipbuilding, 9 Geroyiv Stalingrada Ave., Mykolayiv, 54025, Ukraine

³ National Aviation University, 1 Kosmonavta Komarova Ave., Kyiv, 03680, Ukraine

The need for utilization of a user state model in distance learning systems (DLS) was substantiated. To develop this model, all the DNS teaching material is divided into the sets of elementary indivisible data of specific type, e.g., definitions, explanations, formulas, schemes, theorems, descriptions, etc. A set of data to be mastered by a specific user is formed. With this done, in every subject, the following three types of sets are considered as user states: a set of all learned and checked data, a set of all learned and not yet checked data, and a set of all the marks obtained for tests. Moreover, the system deals with sets of elementary data being checked by specific standard tests and with a set of user's standard actions enabling him/her to change his/her user's state for another one. Based on these values, a graph model for the states of DLS user is formed to match to his learning process.

Keywords: graph, set, electronic learning, distance education

ВИКОРИСТАННЯ СИМВОЛІВ ЯКОБІ ДЛЯ ГЕНЕРУВАННЯ ПАРАМЕТРІВ ЕЛІПТИЧНОЇ КРИВОЇ В КРИПТОСИСТЕМАХ

І.З. Якименко¹, Л.М. Тимошенко², В.А.Мокріцький²

¹ Тернопільський національний економічний університет,
вул. Львівська, 1, м.Тернопіль, 46020, Україна;

² Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна, e-mail: lint0902@gmail.ru

Запропоновано підхід до генерування параметрів еліптичної кривої в криптосистемах на основі генетичного алгоритму та з використанням символів Якобі, розроблено новий алгоритм генерування параметрів та базової точки еліптичної кривої, що дозволив підвищити стійкість алгоритмів шифрування інформації на еліптичних кривих та ефективність захисту інформації в комп'ютерних системах.

Ключові слова: криптосистема, еліптична крива, параметри еліптичної кривої, символ Якобі

Вступ

Інформаційні ресурси в сучасних умовах є одним із найважливіших результатів діяльності людського суспільства, саме тому особлива увага приділяється задачі їх захисту. Чільне місце у вирішенні цієї складної задачі посідає криптографічний захист інформації - вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо (ст. 1 Закону України «Про державну таємницю»).

Всі криптографічні алгоритми з відкритим ключем для розподілу ключів, шифрування інформації спираються на один з наступних типів незворотних перетворень [1]: розклад великих чисел на прості множники, або задача факторизації; проблема дискретного логарифмування; обчислення коренів алгебраїчних рівнянь.

Для надійного захисту інформації в криптосистемі RSA використовуються ключі розрядністю не менше 1024 біт. Захищеність більшості інших алгоритмів з відкритим ключем – Ель-Гамала, DSA тощо ґрунтується на задачі дискретного логарифмування. При оцінці складності операції факторизації чисел і розв'язанні задачі дискретного логарифма показано, що вони вимагають приблизно однакового обсягу роботи [2]. Отже, ключі RSA, Ель-Гамала, DSA однакової довжини будуть мати приблизно однакову стійкість.

Якщо не враховувати вже відомі криптографічно слабкі криві, стійкість алгоритмів шифрування на еліптичних кривих оцінюється як експоненційна [3, 4, 5, 6]. Складність атаки на ключ у цьому випадку експоненційно пов'язана з довжиною ключа, тобто наростає дуже швидко й для деякої довжини ключа атака стає практично нереалізованою. Стійкість же систем шифрування RSA й Ель-Гамала субекспоненційна. Практично це означає, що алгоритми шифрування на еліптичних кривих за однакової стійкості мають розмір ключа на порядок менший, ніж у названих системах. Відомо [7], що еліптична крива із розміром ключа 160 біт забезпечує ту ж

стійкість, що й традиційні системи захисту розмірності ключа 1024 біт. Тому на даний час, по суті, немає альтернативи алгоритмам шифрування на еліптичних кривих.

На сьогодні еліптичні криві застосовують для реалізації різноманітних класів систем захисту інформації, зокрема для побудови симетричних, асиметричних криптосистем та систем електронного цифрового підпису. Незважаючи на вагомі переваги застосування еліптичної кривої (ЕК), існують проблеми, що зумовлюють такі класи задач [2,3]: генерування параметрів еліптичної кривої; обчислення порядку еліптичної кривої; дискретне логарифмування.

Постановка задачі дослідження і мета статті

Задачею генерування параметрів еліптичної кривої вигляду [2]

$$\begin{aligned} y^2 &\equiv x^3 + ax + b \pmod{p}, \quad pF \in F_p, \\ \Delta &= -(4a^3 + 27b^2) \neq 0, \quad a, b \in F_p, \end{aligned} \quad (1)$$

де $(x, y) \in E(F_p) \cup O$, O - нескінченно віддалена точка, є знаходження таких параметрів:

1. Просте число p – модуль перетворення груп точок ЕК, що повинно задовольняти нерівність $p > 2^{255}$. Верхня границя числа визначається конкретною реалізацією криптосистеми. Для створення цифрового підпису довжиною 512 біт, як це було для стандарту ГОСТ 34.310-95, число p повинно задовольняти нерівність $p < 2^{256}$. В подальшому вважаємо, що число p лежить в межах $2^{255} < p < 2^{256}$;

2. Просте число q , яке визначає порядок циклічної підгрупи групи точок еліптичної кривої E [2].

Для генерування простого числа можна використовувати такі процедури:

- генерування числа q в стандарті ГОСТ 34.310-95;
- генерування випадкового простого числа довжиною 256 біт;
- генерування сильного простого числа;
- генерування коефіцієнтів, де $a, b \in GF(p)$, що задають еліптичну криву E .

У [8] запропоновано метод генерування параметрів ЕК, що базується на генетичному підході, який полягає в одержанні за оптимальний час максимально наближеного значення цільової функції [9]. Для його реалізації взято за основу алгоритм А.12.4 стандарту IEEE P1363 [10] і розроблено алгоритм генерування параметрів ЕК з використанням генетичного підходу.

Використано такий критерій на базі наведеного в стандарті співвідношення оцінки гладкості кривої, отриманої на основі виразу

$$f = c \cdot b^2 \pmod{p} - a^3 \pmod{p}, \quad (2)$$

де $a, b \in GF(p)$.

Врахування напряму зміни коефіцієнтів a , b дозволило суттєво підвищити ефективність роботи алгоритму – швидкодія зросла в 1.5-2 рази в залежності від розмірності параметрів a і b відносно алгоритму простого перебору. Зазначимо, що даний алгоритм має функціональні обмеження - простий перебір параметрів (a, b) , хоча і з врахуванням операторів мутації та напрямків зміни коефіцієнтів a , b .

Отже, для підвищення ефективності захисту інформації в комп'ютерних системах та стійкості алгоритмів шифрування інформаційних потоків на еліптичних кривих

потрібен пошук нових підходів, які дозволять пришвидшити алгоритм генерування параметрів ЕК, що і є *метою* даної статті.

Основна частина

Для підвищення швидкодії генерування параметрів ЕК пропонується новий підхід з використанням символів Якобі [11]. Дослідження показали, що це дасть змогу зменшити часовий ресурс і збільшити загальну кількість пар параметрів (a, b) , що генеруються. Символи Якобі дають можливість визначити, чи існує таке h , яке задовольняє рівність, отриману шляхом перетворення виразу (2):

$$h = (c^{-1}(\bmod p)a^3) \bmod p. \quad (3)$$

Згідно властивості символів Якобі [11], якщо $(a/p) = -1$, то $x_2 = a \bmod p$ не має рішення. Завдяки цьому можна відсіювати значення h , для яких символ Якобі дорівнює -1 . Якщо ж символ Якобі дорівнює 1 , то одержуємо

$$b^2 \equiv h(\bmod p) \quad (4)$$

Запропонований алгоритм збільшить швидкість в порівнянні з генетичним алгоритмом пошуку параметрів ЕК за рахунок відсіювання параметрів (a, b) , для яких символ Якобі не дорівнює 1 .

З врахуванням вище сказаного загальний алгоритм генерування параметрів ЕК запишеться наступним чином.

1. Генерування числа c .
2. Генерування випадкового числа a .
3. Обчислення значення h .
4. Знаходження символу Якобі $j = J(h, p)$.
5. Якщо $j = -1$, то перейти до кроку 2.
6. Знаходження числа b .
7. Перехід на крок 1.

Слід зазначити, що при кожному генеруванні нового числа c для кожної пари параметрів ЕК значно зменшується швидкість алгоритму. Блок-схема алгоритму подана на рис. 1.

З використанням наведеного алгоритму розроблено програмний продукт генерування параметрів ЕК для заданого модуля p в середовищі візуального програмування C++ Builder 6.0. Для визначення швидкодії запропонованого алгоритму було згенеровано 10 тисяч пар параметрів ЕК. Загальний час генерування становить 2 хв. 26.58 сек., тобто приблизний час генерування однієї пари дорівнює 14 мс. Варто зазначити, що при визначенні швидкодії число a було 256-бітним, а алгоритм допускає зменшення його розрядності. Тоді швидкість алгоритму буде ще вищою. Програма, розроблена для реалізації поданого алгоритму, була доповнена реалізацією алгоритму генерування базової точки на ЕК. Модуль кривої p було взято з стандарту X9-62 [12]:

$$p = 115792089210356248762697446949407573530086143415290314195533631308867097853951$$

Після доповнення програми генерування параметрів генеруванням точки швидкість виконання алгоритму незначно зменшилася.

В таблиці 1 подано приклад згенерованих параметрів і координат базових точок еліптичної кривої.

Кількість пар, які генеруються, визначає паузу між циклами генерування. Під час генерування параметрів доступу до елементів керування вікном немає, тому після генерування кількості пар, яка задана в вищезазначеному полі, робиться пауза на 100 мс. При заданні дуже малих значень швидкодія програми суттєво зменшиться через велику кількість пауз, під час яких параметри не генеруватимуться. При заданні великих значень швидкодія висока, проте майже не буде доступу до вікна. Оптимальний вибір – 500-1000 пар. Ім'я поля редагування, в якому встановлюється кількість генерованих пар, EFreq. По замовчуванню в цьому полі встановлюється число 500.

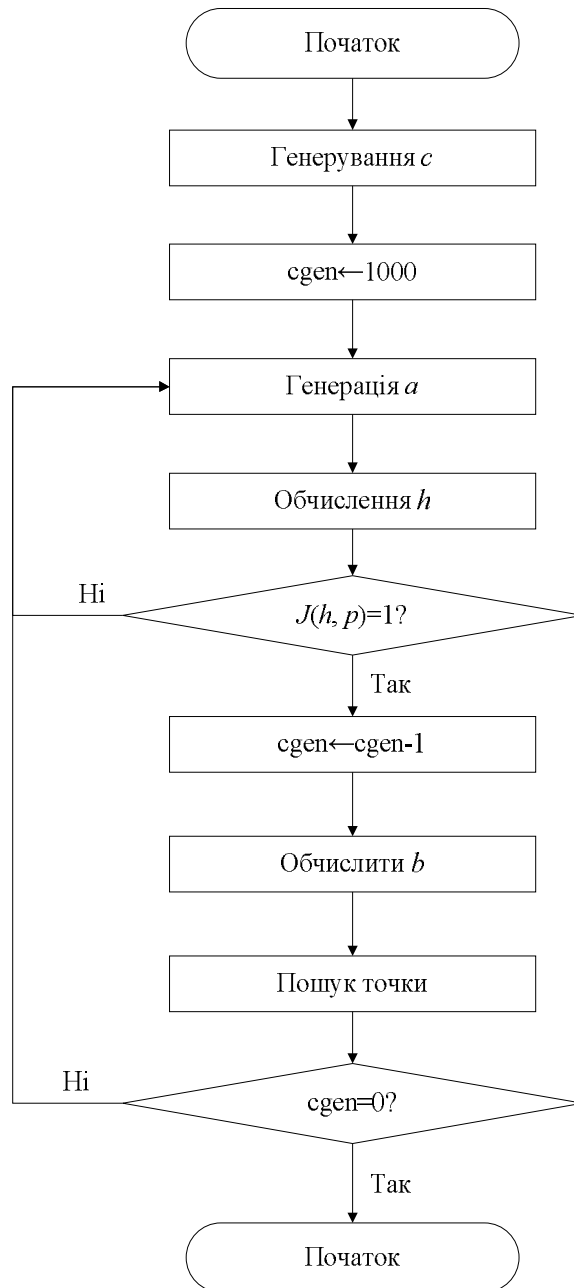


Рис.1. Алгоритм генерування параметрів ЕК з використанням символів Якобі

Проте не завжди потрібно генерувати саме 256-бітне число a . Його розрядність можна змінити, переключившись на змінну розрядність і вказати межі бітності числа a . Якщо потрібне число строгої розрядності (наприклад, 200 біт), то необхідно

встановити однакові значення для максимальної та мінімальної розрядності. Якщо розрядність встановити неправильно, то подається повідомлення, представлене на рис. 2.

Таблиця 1.

Приклад згенерованих параметрів та координат базових точок на ЕК

Число c	Параметри ЕК	Координати точки
$c=4622141082350$ 761958088502957 771218460401318 074586653131924 490106838143083 4019	$a=114696062184921291074865670$ 68054309197980372528558405435 2011807055156770377329 $b=841023222462353149745592116$ 56505809896498381488370328980 244492251701089994880	$x=563421868221961100817039648$ 57654083632130498187698608236 967225088647602140708 $y=454365965925119316295698855$ 64096535284318424274910022081 214046273849647278168
$c=4495282155949$ 033906019773293 755442107970996 262433769553132 698783128445532 2679	$a=624485043717780937523339154$ 66416825250203415860656193403 073976324655346540088 $b=487760277949220977012685921$ 25885615099753604479151430418 547735948440420840414	$x=932732926462204380524923766$ 63941162818585306673620807190 438274113700039002007 $y=-556843238082099176$ 5342879723984285106 45865178119693397205711468572 54294477132
$c=4631150059097$ 348210440033480 198418634575360 382240344739275 695741690967414 4562	$a=694555539263599989359569752$ 07837961345215187825158850426 367316454247044183376 $b=101921245183226147244012099$ 90443502405655683069689431820 7652305979079392107026	$x=961169947263813680823857016$ 74005499394115565542615817795 86275296230817584968 $y=-785024814107883208$ 6782998900642022692058 58180045641255973366754666003 73083457
$c=2587762300678$ 935703451124709 265240616294772 707383432045542 153686871273158 7895	$a=735875671267604836775853578$ 60726059097012187533517473774 145023184880783157813 $b=332063496062754484532058678$ 54697432988301728737300381901 236754438097544091177	$x=727523675521774054958355159$ 61374751940024200546485626335 681266135036309097122 $y=726161820508571658310810441$ 77317019061041565413455809618 410794248932607278083
$c=2181212195678$ 094818479708491 098824025372465 709197803661588 154957091039001 9686	$a=859997439017321900411494888$ 84242181294898484866902415434 124761386757328167530 $b=103615535785767612720472812$ 07511476143254362069691704141 1990013038205060297460	$x=6779257572574225023$ $y=-8462646205002030098020$ 14132751659349153 50944360430106725242471082843 207917740

До вихідних даних програми відносяться згенеровані параметри, число c , координати точки на ЕК із знайденими параметрами, кількість запусків процедури генерації параметрів, символ Якобі для конкретного числа a , кількість знайдених параметрів та час пошуку параметрів.

Числа a, b, c виводяться в поля редагування з іменами ANum, BNum, CNum відповідно. В цих полях властивість ReadOnly встановлена в true, тобто змінювати в них текст користувач не може, але може скопіювати його в буфер обміну ОС Windows.

Всі інші вихідні дані виводяться за допомогою міток (тип TLabel). Їх імена для значень кількості запусків процедури генерації символу Якобі, кількості знайдених пар (a, b) , мітки, яка містить кількість згенерованих пар (для часової характеристики значення кількості пар кратні 500) та мітки, яка містить загальний час генерації, мають значення відповідно CStep, Jac, Couples, LFound, Found.

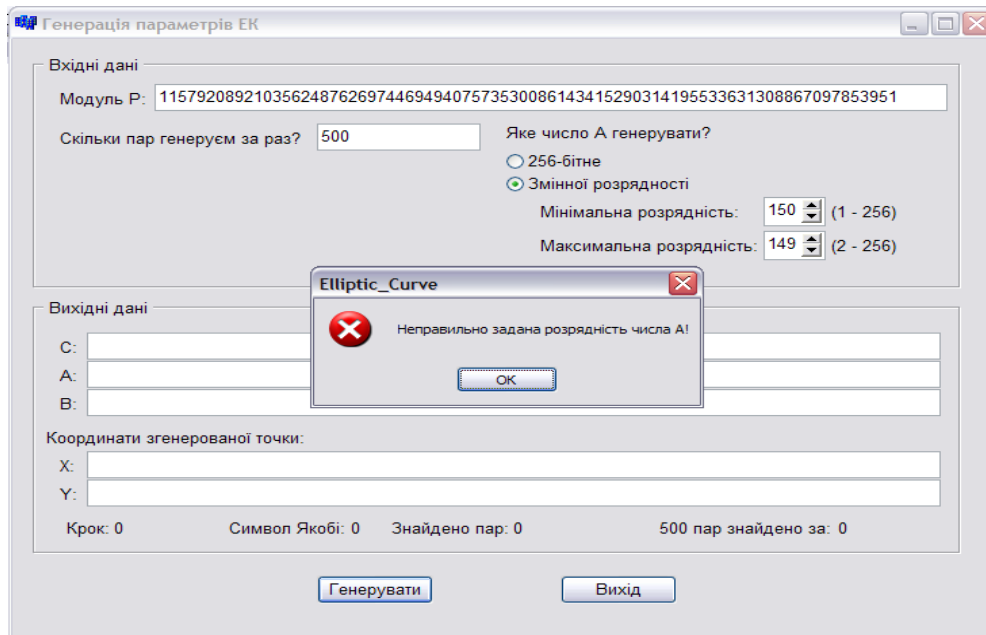


Рис.2. Процес генерування параметра ЕК

Приклад роботи програми для генерації 1200 пар з бітовим коридором для a 120-200 біт подано на рисунку 3.

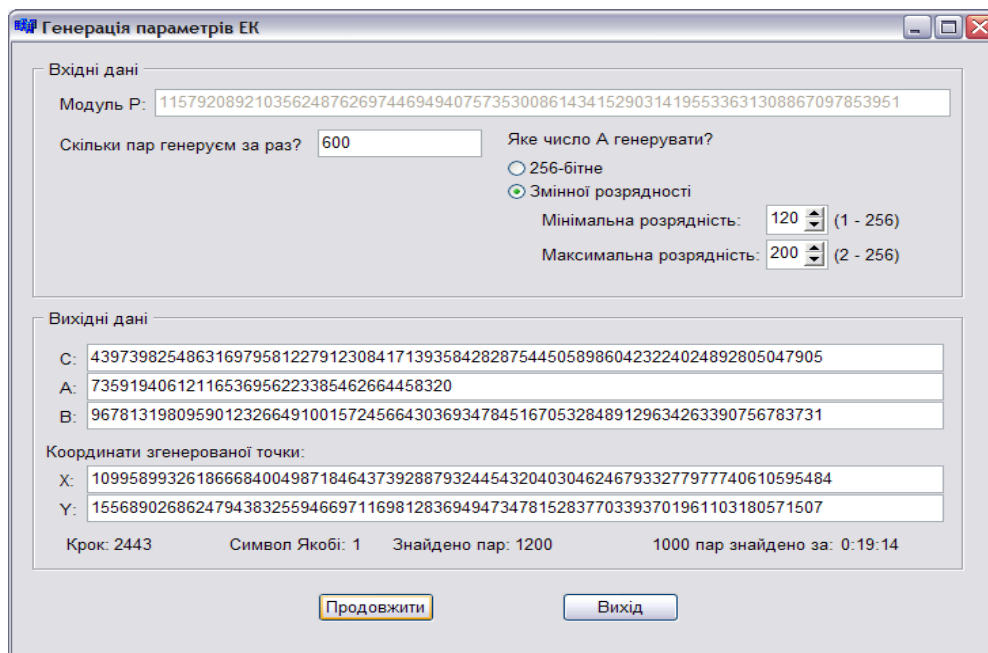


Рис.3. Інтерфейс генерування параметрів та базової точки ЕК

Також вихідні дані виводяться в два файли – Numbers.txt та Time.txt. В перший файл виводяться згенеровані параметри та координати точки. Він програмою ніколи не знищується. В файл Time.txt виводиться часова характеристика. При кожному запуску програми цей файл очищується. Програма використовує зовнішні бібліотеки lpr.c та BigInt.cpp. В першій містяться функції для реалізації алгоритмів, які використовує IEEE P1363 A.12.4 та IEEE P1363 A.11.1. Друга містить функції, які використано для реалізації процедури виконання операцій над числами великої розрядності.

Результати чисельного експерименту генерування параметрів - залежності кількості пар параметрів ЕК від часу генерування наведено в табл. 2.

Аналіз результатів моделювання показав, що підхід з використанням символів Якобі дозволяє пришвидшити час роботи алгоритму в $9.91736 \cdot 10^3$ разів по відношенню до генетичного алгоритму, отже, генерувати параметри еліптичної кривої для побудови систем захисту інформаційних потоків з використанням математичного апарату ЕК майже на чотири порядки швидше, та до шести порядків відносно алгоритму простого перебору.

Таблиця 2.

Часові характеристики роботи програми

Кількість пар (a, b)	Час, s алгоритм з використанням символів Якобі	Час, $10^{-3} s$ Генетичний алгоритм
500	10.89	108.001
1000	21.19	209.1467
1500	31.77	315.0749
2000	42.69	423.2771
2500	53.25	528.0979
3000	63.66	631.3396
3500	74.25	736.3912
4000	84.80	840.9612
4500	95.52	947.1576
5000	106.05	1051.7643

Висновки

Запропонований алгоритм генерування параметрів ЕК на основі використання символів Якобі, розроблений на базі генетичного алгоритму, характеризується суттєвими перевагами швидкодії - приблизно чотири порядки по відношенню до генетичного алгоритму, та до шести порядків відносно алгоритму простого перебору, що є важливою перевагою його застосування для побудови стійких систем захисту інформаційних ресурсів з використанням математичного апарату ЕК.

Список літератури

1. Болотов, А.А. Алгоритмические основы эллиптической криптографии. / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, А.А. Часовских. / – Москва: МЭИ. – 2000. – 100 с.
2. Бессалов, А.В. Криптосистемы на эллиптических кривых: Учеб. пособие. // А.В. Бессалов, А.Б. Телиженко / – К.: ИВЦ «Видавництво «Політехніка»». – 2004. – 224 С.
3. Карпінський, М.П. Еліптична крива для асиметричної криптографічної системи. // М.П. Карпінський, І.З. Якименко, І. Дуда / Вісник Тернопільського державного технічного університету імені Ів. Пулюя, - Том 6, - №3 – 2001. – С:91–95.

4. Карпінський, М.П. Оцінка продуктивності та стійкості до часового аналізу алгоритмів експоненціювання точки еліптичної кривої.// М.П. Карпінський, І.З. Якименко, М. Гіжицькі / Вісник Хмельницького національного університету. – 2006. – № 5. – С. 23-30.
5. Дубчак, Л.О. Оцінка часової реалізації алгоритму Монтгомері // Л.О.Дубчак, Л.М. Тимошенко, Ю.М. Чайківська / Зб.праць міжн. наук.-пр. конф. «Інформаційні технології в економіці, менеджменті і бізнесі. Проблеми науки, практики і освіти» К.: ЄУ,2007.-С.77-78.
6. Дубчак, Л.О. Спосіб вибору методу модулярного експоненціювання для побудови оптимальної системи захисту конфіденційної інформації // Л.О.Дубчак, Л.М. Тимошенко, Т.О. Яремчук / Інформаційна безпека. – Луганськ:, ЛНУ. - 2011. №1(5). - С.112-117.
7. Карпінський, М.П. Оцінка продуктивності та стійкості до часового аналізу алгоритмів експоненціювання точки еліптичної кривої.// М.П. Карпінський, І.З. Якименко, М. Гіжицькі / Вісник Хмельницького національного університету. Х., ТУП. – 2006. – № 5. – С. 23-30.
8. Карпінський, М. Метод генерування параметрів еліптичних кривих. // М. Карпінський, І. Васильцов, І. Якименко, Я. Кінах / Правове, нормативне, та метрологічне забезпечення системи захисту інформації в Україні. К. –2003– № 6.– С.74.
9. Исаев, С. Генетические алгоритмы – эволюционные методы поиска. [Электронный ресурс] // С. Исаев. Режим доступа: http://ai-online.fromru.com/documents-genetic_algorithms.html.
10. IEEE P1363-2000 / D8(Draft Version 8). Standard Specifications for Public Key Cryptography.
11. Айерлэнд, К. Классическое введение в современную теорию чисел.// К. Айерлэнд, М. Роузен/ — М.: Мир.– 1987- 416 с.
12. X9.62-1998. Public Key Cryptography For The Financial Services Industry. Public Key Cryptography For The Financial Services Industry.

ИСПОЛЬЗОВАНИЕ СИМВОЛОВ ЯКОБИ ДЛЯ ГЕНЕРИРОВАНИЯ ПАРАМЕТРОВ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ В КРИПТОСИСТЕМАХ

И. З. Якименко¹, Л. Н. Тимошенко², В.А. Мокрицкий²

¹ Тернопольский национальный экономический университет,
ул. Львовская, 1, г.Тернополь, 46020, Украина;

² Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: lint0902@gmail.ru

Предложено подход генерирования параметров эллиптической кривой в криптосистемах на основе генетического алгоритма и с использованием символов Якоби, разработано новый алгоритм генерирования параметров и базовой точки эллиптической кривой, который позволил повысить стойкость алгоритмов шифрования информации на эллиптических кривых и эффективность защиты информации в компьютерных системах.

Ключевые слова: Криптосистема, эллиптическая кривая, параметры эллиптической кривой, символ Якоби.

USE OF JACOBI SYMBOLS TO GENERATE THE ELLIPTIC CURVE PARAMETERS IN CRYPTOSYSTEMS

I.Z. Yakimenko¹, L.N. Timoshenko², V.A. Mokritskyi²

¹ Ternopil national economical university
1, Lvivska Str., Ternopil, 46020, Ukraine;

² Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: lint0902@gmail.ru

A Jacobi symbols-utilizing approach to generation of elliptic curve parameters in cryptosystems was proposed based on genetic algorithm. A new algorithm to generate the elliptic curve parameters and reference point was developed thereby providing for improvement in both robustness of data coding algorithm based on elliptic curves and efficiency of data protection in computer systems.

Keywords: cryptosystem, elliptic curve, elliptic curve parameters, Jacobi symbol.

МЕТОД РОЗПІЗНАВАННЯ ВИХІДНОГО СИГНАЛУ МУЛЬТИСЕНСОРА ЗА ДОПОМОГОЮ МОДУЛЬНИХ НЕЙРОННИХ МЕРЕЖ

І.В. Турченко

Тернопільський національний економічний університет,
вул. Львівська, 1, Тернопіль, 46020, Україна; e-mail: iryna.turchenko@gmail.com

Розглянуто метод розпізнавання вихідного сигналу мультисенсора за допомогою модульних нейронних мереж. Вихідний сигнал мультисенсора описано за допомогою набору математичних моделей. Математичні моделі розглянуті для випадків, коли характеристики перетворення по фізичних величинах мають додатні похідні, від'ємні похідні, похідні різного знаку при збільшенні та зменшенні амплітуди вихідного сигналу мультисенсора. Підвищення точності розпізнавання підтверджено результатами імітаційного моделювання.

Ключові слова: мультисенсор, розпізнавання, модульні нейронні мережі

Вступ

Останнім часом все більшого поширення набувають сенсори, вихідний сигнал яких навмисно залежить від декількох фізичних величин, так звані багатопараметричні або мультисенсори (МС) [1]. Такі сенсори використовуються для одночасного збору даних про декілька фізичних величинах. При цьому вимірювані величини впливають на всі параметри вихідного сигналу МС. Наприклад, чутливий елемент МС може бути виконаний у вигляді плівки, яка контактує з вимірюваними фізичними величинами. Таку структуру мають сенсори, які використовуються для ідентифікації різних типів забруднень при екологічних дослідженнях, а також сенсори ідентифікації вибухонебезпечних газів [2] в гірничодобувній промисловості. Останні виконані на базі плівки SnO_2 , яка при нагріванні робочим струмом стає чутливою до концентрацій оксиду вуглецю (CO) і метану (CH_4). Вихідною величиною цих сенсорів є провідність, значення якої залежать від обох фізичних величин. Тому виникає завдання ідентифікації інформації, що знаходиться у вихідному сигналі МС, з метою визначення значень окремих фізичних величин. Точне визначення значень фізичних величин дозволить підвищити достовірність даних, що надходять користувачеві від системи збору та обробки сенсорних даних. Іншими словами, маючи один вихідний сигнал МС необхідно визначити, яка складова його сигналу характеризує кожен окрему фізичну величину. Тому фізичний зміст цього завдання зводиться до відомої в теорії обробки даних задачі розпізнавання образів.

Методи розпізнавання вихідних сигналів МС розроблялися багатьма вченими. Дедре [3] здійснив якісний аналіз методів класифікації, популярних в загальній хімометрії, наприклад, методи гнучкого незалежного моделювання аналогій класу (soft independent modeling of class analogy – SIMCA) та дискримінантного лінійного аналізу (linear discriminate analysis - LDA). Основні висновки цієї роботи полягають у тому, що: по-перше, вибір кращого алгоритму розпізнавання сильно залежить від сфери застосування, та, по-друге, кращі результати забезпечуються застосуванням змішаних підходів. Найбільш повний аналіз алгоритмів розпізнавання вихідних сигналів МС

хімічних величин [4] включає 23 методи розпізнавання, що базуються на машинному навчанні, статистичних та нейромережових підходах, а також їх якісне та кількісне порівняння. Результат цього аналізу зводиться до того, що нейромережові методи дають найкращі результати, однак вимагають довгого часу навчання та інтуїції експерта-дослідника для їх цілеспрямованого застосування. Як показано в [5], нейромережові методи показують кращі результати в порівнянні з іншими математичними підходами завдяки узагальнюючим властивостям нейронних мереж (НМ), що шляхом самонавчання можуть найбільш оптимально налаштовуватися на вирішувану задачу.

Однак розглянуті вище відомі рішення здійснюють розпізнавання на основі даних, отриманих від масиву сенсорів (sensors arrays). Це призвело до використання дуже складних архітектур НМ, що містять 8 і більше нейронів у вхідному шарі, 16 і більше нейронів у прихованому шарі. На відміну від згаданих методів, метою даної статті є дослідження ефективності найбільш відомої нейромережової парадигми - багатошарового персептрону з алгоритмом навчання зворотного поширення помилки. Його вивченість та хороше сходження алгоритмів навчання [6-7] робить його привабливим для широкого використання, зокрема, в системах реального часу на базі мікроконтролерів. Цей підхід буде застосований для розпізнавання вихідного сигналу одного МС у двох режимах його роботи для підвищення достовірності розпізнавання двох фізичних величин - концентрацій оксиду вуглецю (CO) і метану (CH₄). Таке завдання є надзвичайно важливим для шахтних вентиляційних мереж [8].

Математичні моделі вихідного сигналу мультисенсора

У зв'язку з відсутністю нормованих характеристик перетворення (ХП) МС провести прямі дослідження нейромережових методів розпізнавання не є можливим. Тому для вирішення поставленого завдання, доцільно розробити математичну модель МС. Така модель може бути розроблена на основі аналізу ХП широко використовуваних газових сенсорів типу TGS. Як прототип для побудови математичної моделі був обраний сенсор TGS-813 [9]. У таблиці 1 представлені результати дослідження індивідуальної ХП цього МС, виконані в рамках спільного польсько-грецького дослідницького проекту в Сілезькому вугільному басейні [10]. Для забезпечення розпізнавання обох вхідних величин використовувалися 2 режиму роботи МС, що перемикалися шляхом зміни напруги джерела живлення. При різних напругах живлення МС має різні ХП. В комірках таблиці вказані значення провідності МС (у мікро Сіменсах), що відповідають зазначеним у заголовках значенням концентрацій CO і CH₄. У чисельнику кожної комірки таблиці вказано значення провідності для напруги живлення 4 вольт, у знаменнику - для 5 вольт. Дані таблиці підтверджують висновок про істотну нелінійність ХП МС по обом вхідним величинам.

Таблиця 1.

Значення провідності МС TGS-813 при різних концентраціях CO та CH₄

$C_{CO} \backslash C_{CH_4}$	0	0.05%	0.1%	0.15%	0.2%
0	21.6 / 24.4	52.5 / 31.7	70.7 / 35.3	85.3 / 43.5	95.9 / 44.9
0.05%	28.2 / 43.3	58.8 / 45.3	75.2 / 58.2	87.7 / 60.5	96.4 / 51.1
0.1%	34.5 / 64.5	66.7 / 65.6	81.0 / 73.8	91.3 / 75.7	98.3 / 77.4
0.15%	45.3 / 96.1	75.6 / 100.3	87.2 / 103.8	95.3 / 106.3	100.6 / 108.7
0.2%	61.0 / 134.0	84.1 / 134.8	93.0 / 136.8	100.0 / 138.6	102.9 / 140.2

Однак забезпечення розпізнавання значень окремих фізичних величин (концентрацій газів) нейронними мережами на прикладі характеристик перетворення одного конкретного МС не вирішує питання можливості та доцільності застосування НМ для вирішення цього завдання в загальному випадку. Тому необхідна розробка узагальненої математичної моделі МС, що забезпечує дослідження можливості застосування нейромережевої парадигми для сімейства МС, виконаних за тонкоплівкової технології SnO₂. Таким чином, з даних таблиці 1 необхідно зробити висновок про загальний характер поверхонь, що описують ХП МС та можливості їх варіацій [11]. Слід враховувати, що необхідно моделювати одночасно два варіанти ХП, що відповідають двом режимам роботи МС. Аналіз технічної документації та результатів дослідження різних типів МС показує, що можливі наступні поєднання параметрів математичних залежностей, що моделюють ХП МС:

1. ХП МС у двох режимах роботи мають по першій фізичній величині додатні перші і другі похідні, а по другій - від'ємну першу і додатну другу похідні;
2. ХП МС у двох режимах роботи мають по першій фізичній величині додатні перші і від'ємну другу похідні, а по другій - від'ємну першу і другу похідні;
3. ХП МС в першому режимі роботи мають по першій фізичній величині додатну першу і від'ємну другу похідні, а по другій - від'ємну першу і другу похідні. У другому режимі роботи ХП МС мають по обох фізичних величинах від'ємну першу і другу похідні;
4. ХП МС в першому режимі роботи мають по першій фізичній величині додатні першу і другу похідні, а по другій - від'ємну першу і додатну другу похідні. У другому режимі - по першій фізичній величині додатну першу і від'ємну другу похідні, а по другій - від'ємні першу і другу похідні. При цьому ХП в обох режимах роботи перетинаються.

Чисельний аналіз показав, що такі ХП можуть бути про імітовані за допомогою добутку двох поліномів різного порядку з різними коефіцієнтами [11]:

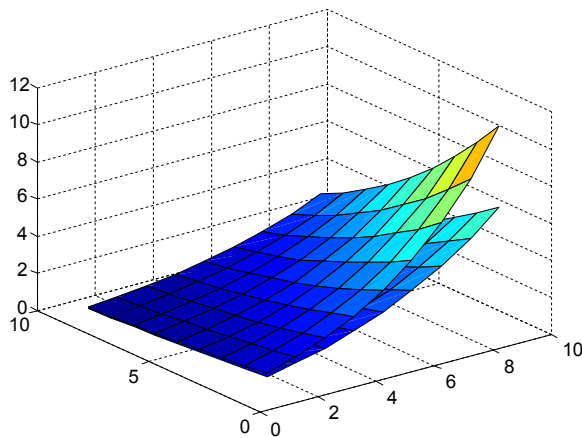
$$Y = (A \times (X_1 + B)^k + C \times (X_1 + B)) \times (D \times (X_2 + E)^l + F \times (X_2 + E)) \times G,$$

де

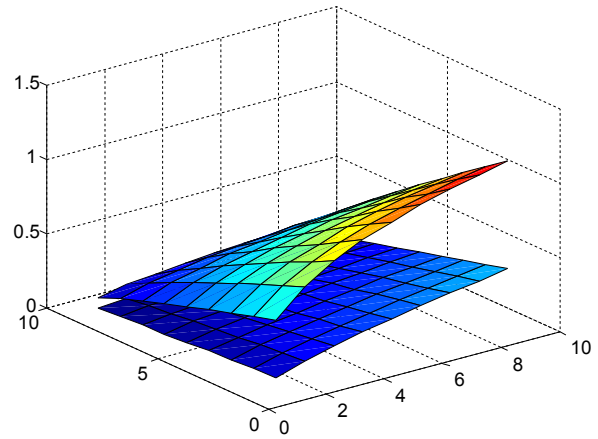
X_1 і X_2 - концентрації СО і СН₄,

B, E - зміщення, що враховують початковий опір МС.

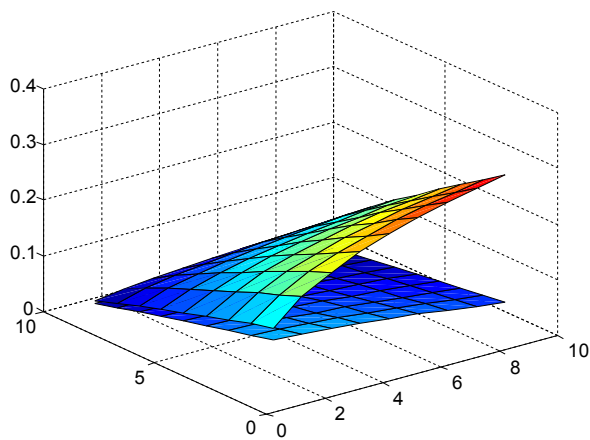
Всі зазначені вище чотири варіанти ХП МС реалізуються зміною значень і полярності коефіцієнтів A, B, C, D, E, F, G і показників ступеня k і l [12]. Зображення поверхонь, що відповідають варіантам (1)...(4), представлені на рис. 1. Найбільш адекватною ХП МС TGS-813 є модель (2), так як значення вихідного сигналу МС росте (перша похідна додатна), а швидкість росту сповільнюється (друга похідна від'ємна). Однак ХП МС можуть змінюватися в досить широких межах. Тому необхідно дослідити можливості розпізнавання вихідного сигналу МС для згаданих вище чотирьох варіантів, що відображають граничні відхилення ХП від номінальних. На рис. 1 верхні поверхні описують ХП МС в першому режимі роботи, нижні - в другому режимі роботи. Значення по осях рис. 1 представлені в умовних одиницях. Для формування вибірок навчання НС ці поверхні були спроектовані на вісь ординат таким чином, що по осі ординат відкладені значення вихідного сигналу МС в першому і в другому режимах роботи, а по осі абсцис - відповідні їм значення двох вхідних фізичних величин.



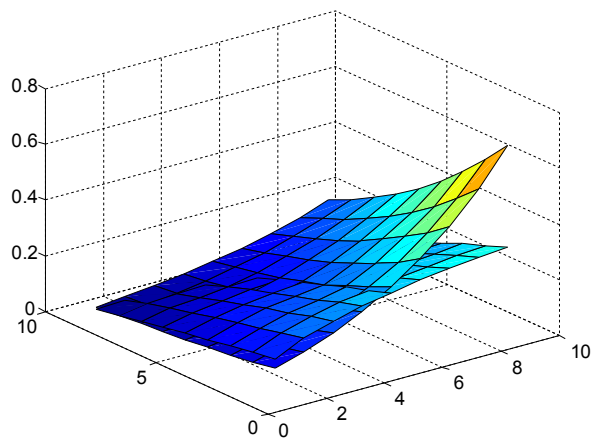
а



б



в



г

Рис. 1. Математичні моделі вихідного сигналу МС: а – для варіанту (1); б – для варіанту (2); в – для варіанту (3); г – для варіанту (4)

Метод модульних нейронних мереж для розпізнавання сигналу мультисенсора

Серед відомих структур НМ, які вирішують задачі розпізнавання значень фізичних або хімічних величин на основі сенсорних даних, доцільно вибрати просту модель багатошарового персептрона враховуючи його хороші узагальнюючі властивості і додатний досвід застосування іншими дослідниками [4]. Кількість нейронів вихідного шару НМ має відповідати кількості вхідних фізичних величин МС і дорівнює двом. Кількість нейронів вхідного шару НМ визначається кількістю режимів роботи НМ, що також дорівнює двом. Кількість нейронів прихованого шару має бути достатнім для забезпечення необхідної точності розпізнавання. Однак надмірне збільшення цієї кількості може призвести до погіршення узагальнюючих властивостей НМ [6]. Для проведення досліджень використана гетерогенна НМ з різними функціями активації нейронів в прихованому і вихідному шарах. У порівнянні з гомогенними (функції активації нейронів в шарах однакові), гетерогенні НМ забезпечують кращу здатність до навчання (універсальність) на різних даних за рахунок застосування функцій активації різної природи. У гетерогенних НМ для навчання доцільно використовувати алгоритм багаторазового поширення помилки (multiple propagation

error) [7], який є модифікацією алгоритму зворотного поширення помилки [6] (back propagation error) шляхом налаштування вагових коефіцієнтів тільки одного шару на кожному кроці навчання. Цей алгоритм дозволяє підвищити стабільність процесу навчання НМ за рахунок усунення явища розсинхронізації навчання для шарів НМ з різними функціями активації [7].

Отримані результати імітаційного моделювання методу розпізнавання за допомогою одномодульної НМ [11, 12] показали середнє і максимальне відносне відхилення розпізнавання 1% і 8% для першої фізичної величини і 5% і 18% для другої фізичної величини. Похибка 5% і вище не задовольняє вимоги безпеки шахтних вентиляційних мереж - концентрація метану 1.5% є вибухонебезпечною, при якій все обладнання має бути вимкнене, а люди евакуйовані з небезпечних ділянок [8].

Широко відомим прийомом підвищення точності вимірювань є розбиття широкого діапазону вхідних сигналів на ряд піддіапазонів. По відношенню до методу розпізнавання за допомогою НМ розбиття на діапазони означає використання окремої НМ для кожного піддіапазону. У теорії НМ такий підхід називається модульними нейронними мережами [13]. При цьому велике або багатопараметричне завдання розбивається на ряд елементарних завдань, вирішується окремими НМ з незалежними вибірками навчання, а приватні рішення об'єднується в один результат. Використовувати цей підхід дозволяє відсутність взаємозв'язку між значеннями вихідного сигналу МС і вихідними фізичними величинами в окремих піддіапазонах.

Згідно з методом розпізнавання вихідного сигналу МС за допомогою модульних НМ (рис. 2), вся вибірка навчання (81 вектор) розділена на три підвибірки розміром 27 навчальних векторів. Відповідно оригінальна вибірка тестування (576 векторів) також розділена на три підвибірки розміром 192 вектора. Кожен модуль НМ функціонував окремо, здійснюючи розпізнавання вихідного сигналу МС у своєму діапазоні.

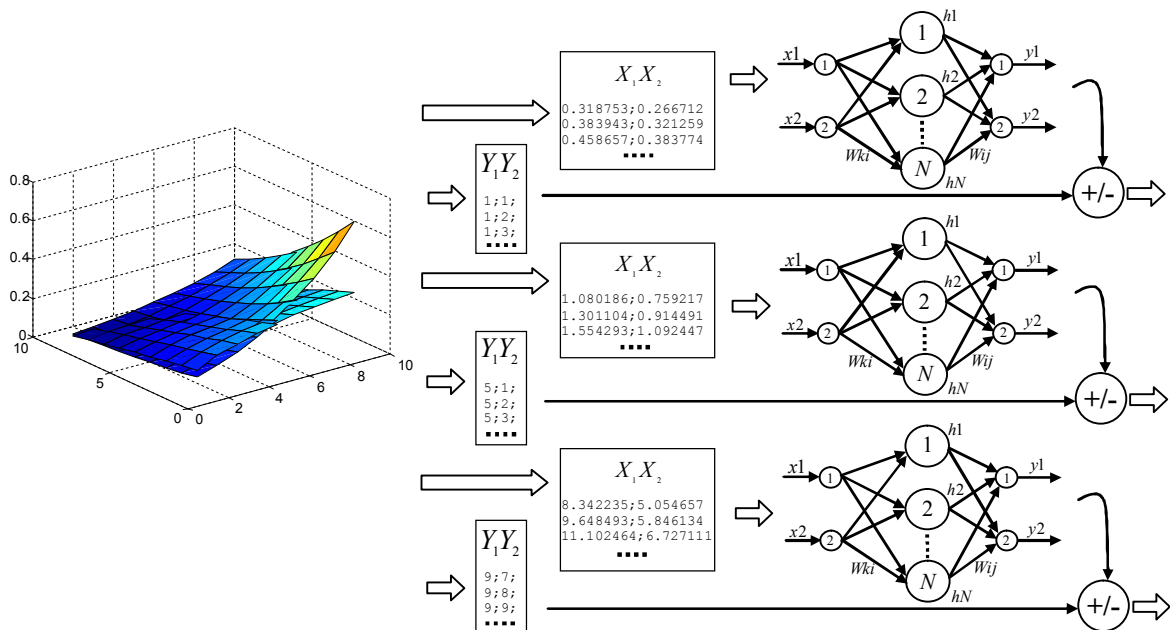


Рис. 2. Метод розпізнавання вихідного сигналу МС модульними НМ

Імітаційне моделювання методу

Для імітаційного моделювання використано середовище MATLAB 6.5. Кожен модуль НМ складався з 2 нейронів вхідного і 2 нейронів вихідного шару. Згідно з

результатами попередніх експериментальних досліджень найвищу точність розпізнавання при застосуванні одномодульної НМ забезпечує архітектура з 10 нейронами прихованого шару [11, 12]. Були досліджені усереднені по чотирьох математичних моделях залежності максимального і середнього відносного відхилення розпізнавання обох фізичних величин. Дослідження проводилися при зміні значення сумарної середньоквадратичної помилки навчання НМ (4) до значень 10^{-2} , 10^{-3} , 10^{-4} та 10^{-5} . Результати імітаційного моделювання по розпізнаванню двох фізичних величин згідно з методом модульної НМ наведено на рис. 3. Як видно, при навчанні НМ до значення середньоквадратичної помилки 10^{-5} , метод модульних НМ забезпечує середнє і максимальне відносні відхилення розпізнавання менше 1% і 2% відповідно, що дозволяє говорити про достатню точність запропонованого підходу. Таким чином, метод розпізнавання за допомогою модульних НМ показав зменшення максимального відносного відхилення розпізнавання в 5-10 разів, а середнього відносного відхилення розпізнавання в 3-4 рази в порівнянні з методом одномодульної НМ.

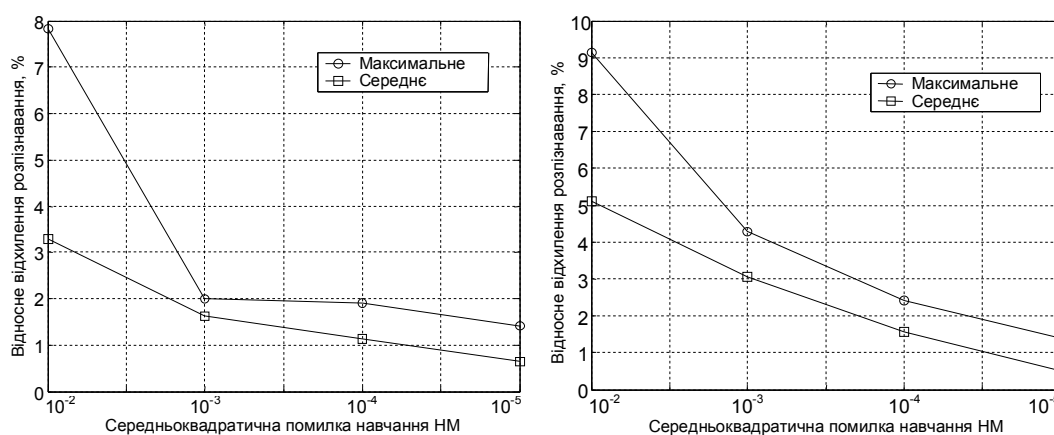


Рис. 3. Результати розпізнавання двох фізичних величин методом модульних НМ

Висновки

Згідно з наведеними вище результатами досліджень можна зробити висновок про перспективність застосування модульних нейронних мереж для розпізнавання вихідних сигналів мультисенсорів. Практичне застосування описаного методу розпізнавання фізичних величин можливо, в першу чергу, для розпізнавання концентрацій шкідливих газів CO і CH_4 в аерогазовому середовищі вугільних шахт з метою запобігання аварійних ситуацій. Крім того, даний підхід може бути адаптований для роботи в автомобільних тунелях, метрополітенах, в інших підземних або закритих приміщеннях, де безпека людей є надзвичайно важливим фактором.

Список літератури

1. Taner, A.H. Virtual instrumentation and intelligent sensors / A.H. Taner, J.E. Brignell // *Sensors and Actuators A: Physical*. – 1997. – Vol. 61, No. 1-3. – P. 427-430.
2. Capone, S. Analysis of CO and CH_4 gas mixtures by using a micromachined sensor array / S. Capone, P. Siciliano, N. Bârsan, U. Weimar, L. Vasanelli // *Sensors and Actuators B: Chemical*. – 2001. – Vol. 78, No. 1-3. – P. 40-48.
3. Derde, M.P. Supervised pattern recognition: the ideal method? / M.P. Derde, D.L. Massart // *Analytica Chimica Acta*. – 1986. – Vol. 191. – P. 1-16.

4. Michie, D. Machine Learning, Neural and Statistical Classification / D. Michie, D.J. Spiegelhalter, C.C. Taylor – New York: Ellis Horwood, 1994.
5. Shaffer, R. E. A comparison study of chemical sensor array pattern recognition algorithms / R.E. Shaffer, S.L. Rose-Pehrsson, A.R. McGill // *Analytica Chimica Acta*. – 1999. – Vol. 384, No. 3. – P. 305-317.
6. Хайкин, С. Нейронные сети: полный курс, 2-е издание / С. Хайкин: Пер. с. англ. – Под. ред. Куссуль Н.Н. – М.: Издательский дом «Вильямс», 2006. – 1104 с.
7. Головкин, В.А. Нейронные сети: обучение, модели и применение / В.А. Головкин. – М.: Радиотехника, 2001. – 256 с.
8. Абрамов, Ф.А. Моделирование динамических процессов рудничной аэрологии / Ф.А. Абрамов, Л.П. Фельдман, В.А. Святный. – К.: Наукова думка, 1981. – 284 с.
9. TGS 813 – for the detection of Combustible Gases: Product information [Електронний ресурс] / Figaro. Режим доступу: <http://www.figarosensor.com/products/813pdf.pdf>
10. Zakrzewski, J. Improving Sensitivity and Selectivity of SnO₂ Gas Sensors by Temperature Variation / J. Zakrzewski, W. Domanski, P. Chaitas and Th. Laopoulos // *IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*. – 2003. – Lviv, Ukraine. – P. 296-299.
11. Turchenko, I. Recognition of MPS Output Signal Described by Different Mathematical Models / I. Turchenko, V. Kochan, A. Sachenko // *Proceedings of the 3rd IEEE International Workshop of Intelligent Data Acquisition and Advanced Computing Systems: Technology and Application (IDAACS'05)*. – 2005. – Sofia (Bulgaria). – P. 89-94.
12. Турченко, И.В. Нейросетевые методы распознавания выходного сигнала мультисенсора / И.В. Турченко, В.В. Кочан, А.А. Саченко // *Вимірювальна та обчислювальна техніка в технологічних процесах*. – 2011. – №2. – С. 137-144.
13. Happel, B. Design and evolution of modular neural network architectures / B. Happel, J. Murre // *Neural Networks*. – 1994. – Vol. 7. – P. 985-1004.

МЕТОД РАСПОЗНАВАНИЯ ВЫХОДНОГО СИГНАЛА МУЛЬТИСЕНСОРА С ПОМОЩЬЮ МОДУЛЬНЫХ НЕЙРОННЫХ СЕТЕЙ

И.В. Турченко

Тернопольский национальный экономический университет,
ул. Львовская, 1, г.Тернополь, 46020, Украина; e-mail: iryna.turchenko@gmail.com

Метод распознавания выходного сигнала мультисенсора с помощью модульных нейронных сетей рассмотрен в этой статье. Выходной сигнал мультисенсора описан с помощью набора математических моделей. Математические модели рассмотрены для случаев, когда характеристики преобразования по физическим величинам имеют положительные производные, отрицательные производные, производные различного знака при увеличении и уменьшении амплитуды выходного сигнала мультисенсора. Повышение точности распознавания подтверждено результатами имитационного моделирования.

Ключевые слова: мультисенсор, распознавание, модульные нейронные сети.

A METHOD TO IDENTIFY A MULTISENSOR OUTPUT SIGNAL BY MEANS OF MODULAR NEURAL NETWORKS

I.V. Turchenko

Ternopil national economical university
1, Lvivska Str., Ternopil, 46020, Ukraine; e-mail: iryna.turchenko@gmail.com

In this paper, a method to identify a multisensor output signal by means of modular neural networks was discussed. A multisensor output signal was defined by mathematical modeling. Mathematical models were considered for the instances when physical quantities transformation characteristics have positive derivatives, negative derivatives, and both positive and negative derivatives for the increase and decrease in the amplitude of multisensor output signal. The improvement in accuracy of identification was confirmed by the results of simulation modeling.

Keywords: multisensory, identification, modular neural networks

МАТЕМАТИЧНІ МОДЕЛІ ТА УЗАГАЛЬНЕННЯ МАТЕМАТИЧНОГО ОПИСУ ПРОЦЕСІВ ПЕРВИННОЇ ПЕРЕРОБКИ СИРИХ ВУГЛЕВОДНІВ

Ю. В. Григоренко

Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна, e-mail: ygrygorenko@lukoil.com

Розроблено математичні моделі процесів та апаратів первинної переробки сирих вуглеводнів, а також виконано узагальнення цих моделей з метою типізації та уніфікації математичного опису класу процесів. Такого роду типізація дає змогу здійснити формалізацію та уніфікацію методів та засобів математичного моделювання і запровадити машинну реалізацію вказаних методів на єдиній уніфікованій основі.

Ключові слова: первинна переробка сирих вуглеводнів, математичні моделі, методи та засоби математичного моделювання

Вступ

Розв'язок задачі математичного моделювання, насамперед і в значній мірі, визначається обраною математичною моделлю (ММ) об'єкту (або процесу). Адекватно обрана ММ забезпечує достовірність результатів математичного моделювання. Крім того, на результати математичного моделювання (зокрема, його точність) впливають чисельні методи, якими реалізується обрана ММ об'єкту (процесу). Тому розробка ММ, що задовольняють вказаним критеріям, дозволяє підвищити ефективність здійснення технологічних процесів.

Основна частина

У відповідності до промислових технологій, при первинній переробці сирих вуглеводнів (ППСВ) запроваджуються такі технологічні процеси: зневоднення, знесолення та первинне відбензинювання, причому перші два процеси виконуються по схемі електро-(термо)знесолення та зневоднення. За фізико-хімічними явищами, які відбуваються, процеси ППСВ (на прикладі типової технологічної схеми первинної переробки сирої нафти [1]) можна класифікувати відповідно як:

- процеси поверхневого теплообміну, в яких теплообмін здійснюється на поверхні розділу окремих реагентів (фаз). Ці процеси відбуваються у таких технологічних апаратах: утилізаційні теплообмінники, теплообмінники газової фракції, теплообмінники дизельної фракції, теплообмінники обтяженої дизельної фракції;
- процеси об'ємного теплообміну, в яких теплообмін здійснюється в межах всього об'єму задіяних реагентів. Ці процеси відбуваються у таких технологічних апаратах: термодегідратори, електродегідратори та змішувачі;
- процеси розсередженого теплообміну, в яких теплообмін одночасно відбувається на декількох окремих поверхнях. Ці процеси відбуваються у таких

технологічних апаратах: колоні попереднього відбензинування, колоні газової фракції, колоні дизельної фракції.

Розробимо ММ наведених класів процесів ППСВ (і відповідних технологічних апаратів, в яких ці процеси відбуваються) та виконаємо їх узагальнення з метою типізації та уніфікації математичного опису. Це має на меті, в подальшому, виконати формалізацію та уніфікацію методів та засобів математичного моделювання, а також здійснити машинну реалізацію зазначених методів на єдиній уніфікованій основі.

Апарати поверхневого теплообміну

Типовим прикладом апарату поверхневого теплообміну є утилізаційний теплообмінник. Він має циліндричну форму порожнини, в якій нагрівається сира нафта. Ця порожнина радіусу r та висотою z характеризується площиною поперечного перетину порожнини S_n (округленнями у верхній та нижній частині конструкції теплообмінника для простоти можна знехтувати), а також висотою h стовпа сирової нафти. У парову порожнину теплообмінника надходить повітря з температурою $T_n = T_n(t)$, нагріте за рахунок утилізації тепла верхнього циркуляційного зрошення та обтяженої дизельної фракції колони попереднього відбензинування. Потік утилізаційного повітря на нагрів визначається витратою F_n , яка, в загальному випадку, також є функцією часу $F_n = F_n(t)$. На вхід теплообмінника надходить сира нафта з температурою $T_{ex} = T_{ex}(r, z, t)$ та витратою $F_{ex} = F_{ex}(t)$. Вихідний потік F_{en} характеризується температурою $T_{en} = T_{en}(r, z, t)$. Потік F_{en} залежить від висоти стовпа сирової нафти в теплообміннику: $F_{en}(h) = K h^{1/2}$, що зумовлено його конструкцією [1].

З урахуванням зазначеного вище, запишемо рівняння матеріального та енергетичного балансів для утилізаційного теплообмінника у диференціальній формі:

$$S_n \frac{\partial h(r, z, t)}{\partial t} = F_{ex}(t) - F_{en}(h), \quad (1)$$

$$\rho C_p S_n \left\{ \frac{\partial [h(r, z, t) T_{en}(r, z, t)]}{\partial t} \right\} = \rho C_p [F_{ex}(t) T_{ex}(r, z, t) - F_{en}(h) T_{en}(r, z, t)] \quad (2)$$

з початковими

$$F_{ex}(t)|_{t=0} = F_{ex_0}, \quad F_{en}(t)|_{t=0} = F_{en_0}, \quad T_{ex}(r, z, t)|_{t=0} = T_{ex_0}, \quad T_{en}(r, z, t)|_{t=0} = T_{en_0} \quad (3)$$

та граничними умовами

$$h(r, z, t)|_{z=0} = 0, \quad T_{en}(r, z, t)|_{z=0} = T_{en}(r, 0, t), \quad \left. \frac{\partial h(r, z, t)}{\partial r} \right|_{r=0} = 0, \quad \left. \frac{\partial T_{en}(r, z, t)}{\partial r} \right|_{r=0} = 0, \quad (4)$$

$$\left. \frac{\partial h(r, z, t)}{\partial r} \right|_{r=r_{\max}} = 0, \quad \left. \frac{\partial T_{en}(r, z, t)}{\partial r} \right|_{r=r_{\max}} = \alpha [T_n(t) - T_{en}(r, z, t)],$$

де ρ, C_p, α — відповідно густина та теплоємність сирової нафти (середні значення), а також коефіцієнт теплопередачі від стінки парової порожнини до нагрівальної (технологічної) порожнини.

Рівняння (1) — (4) утворюють ММ апаратів поверхневого теплообміну процесів ППСВ. Причому, рівняння (1) та (2) являють собою рівняння динаміки, а (3) та (4) — відповідно задають початкові та граничні умови.

Апарати об'ємного теплообміну

Апарати даного класу, в силу особливостей технологічного призначення, відрізняються конструктивним виконанням. Тому виконаємо окремо розробку їх ММ з урахуванням часткових конструктивних особливостей.

Змішувачі. Змішувачі призначено [1] для змішування потоків сирої нафти та води, що використовується для промивки (промивною водою), відповідно перед термодегідраторами та електродегідраторами. Спрощено змішувач являє собою горизонтально орієнтований циліндр. Вхідний потік попередньо нагрітої сирої нафти характеризується температурою $T_{mn} = T_{mn}(t)$ та фіксованою витратою $F_{mn} = \text{const}$. Вхідний потік промивної води характеризується температурою $T_{ne} = T_{ne}(t)$ та регульованою (змінною) витратою $F_{ne} = F_{ne}(t)$. Збудженням є вихідний потік водо-нафтової емульсії із змішувача, який, в свою чергу, характеризується температурою $T_e = T_e(r, z, t)$ та регульованою витратою $F_e = F_e(t)$. Температура водо-нафтової емульсії $T_e = T_e(r, z, t)$ являє собою нестационарну розподілену функцію параметрів r і z , що мають відповідно фізичний зміст відстані від осі змішувача до «дзеркала» водо-нафтової емульсії у змішувачі та довжини змішувача (закругленнями з правого та лівого боку змішувача для простоти можна знехтувати). Висота шару емульсії h визначається наступним чином

$$h = \begin{cases} r_{\max} - r, & \beta = -(\pi/2); \\ r_{\max}, & \beta = 0; \\ r_{\max} + r, & \beta = (\pi/2). \end{cases}$$

З урахуванням зазначеного вище, запишемо рівняння матеріального та енергетичного балансів для змішувача у диференційній формі:

$$S_n \frac{\partial h(r, z, t)}{\partial t} = F_{mn}(t) + F_{ne}(t) - F_e(t), \quad (5)$$

$$\rho C_p S_n \left\{ \frac{\partial [h(r, z, t) T_e(r, z, t)]}{\partial t} \right\} = \rho C_p [F_{mn}(t) T_{mn}(t) + F_{ne}(t) T_{ne}(t) - F_e(t) T_e(t)] \quad (6)$$

з початковими

$$\begin{aligned} F_{mn}(t)|_{t=0} &= F_{mn_0}, \quad F_{ne}(t)|_{t=0} = F_{ne_0}, \quad F_e(t)|_{t=0} = F_{e_0}, \\ T_{mn}(t)|_{t=0} &= T_{mn_0}, \quad T_{ne}(t)|_{t=0} = T_{ne_0}, \quad T_e(r, z, t)|_{t=0} = T_{e_0} \end{aligned} \quad (7)$$

та граничними умовами

$$\begin{aligned}
h(r, z, t)|_{r=0} &= r_{\max}, \quad T_e(r, z, t)|_{r=0} = T_e(0, z, t), \\
h(r, z, t)|_{r_{\max}=0} &= 0, \quad T_e(r, z, t)|_{r_{\max}=0} = T_e(r_{\max}, z, t), \\
\frac{\partial h(r, z, t)}{\partial r}|_{r=0} &= 0, \quad \frac{\partial T_e(r, z, t)}{\partial r}|_{r=0} = 0, \quad \frac{\partial h(r, z, t)}{\partial r}|_{r=r_{\max}} = 0, \quad \frac{\partial T_e(r, z, t)}{\partial r}|_{r=r_{\max}} = 0,
\end{aligned} \tag{8}$$

де ρ, C_p — відповідно густина та теплоємність нагрітої сирової нафти (середнє зважене значення для виходів теплообмінників), S_n — подовжній перетин порожнини змішувача.

Останні чотири рівняння в (8) свідчать про те, що в граничних точках змін відповідних градієнтів висоти та температури шару емульсії немає. Таким чином, рівняння (5) — (8) задають ММ змішувачів нагрітої сирової нафти та промивної води, причому рівняння (5) та (6) є рівняннями динаміки, а (7) та (8) — початковими та граничними умовами, відповідно.

Термодегідратори та електродегідратори. Термодегідратори та електродегідратори призначено для знесолення та зневоднення сирової нафти. При цьому в термодегідраторах відбувається термохімічна обробка водо-нафтової емульсії (відділення знесоленої сирової нафти від промивної води), а в електродегідраторах руйнування водо-нафтової емульсії здійснюється за рахунок електричного поля. Якщо абстрагуватися від способу руйнування водо-нафтової емульсії, то, з точки зору конструктивного виконання, термодегідратори та електродегідратори виконано за аналогічною схемою. Тому, при розробці ММ цих апаратів, розглянемо лише термодегідратор, а отриманий результат поширимо на електродегідратори.

За спрощеною схемою термодегідратор являє собою вісесеметричний горизонтально орієнтований циліндр довжиною z (закругленнями з правого та лівого боку термодегідратора для простоти можна знехтувати) і характеризується одним вхідним та двома вихідними потоками. Вхідний потік утворюється водо-нафтовою емульсією з регульованою витратою $F_e = F_e(t)$, яка надходить до термодегідратора зі змішувача при температурі $T_e = T_e(t)$ (зазначимо, що розподіленість температури T_e , очевидно, повинна розглядатися лише в межах порожнини змішувача). Перший вихідний потік утворює знесолена сира нафта при витраті $F_{zn} = F_{zn}(t)$ та температурі $T_{zn} = T_{zn}(r, z, t)$. Другий вихідний потік утворює промивна вода, яка накопичується в нижній частині термодегідратора при термохімічному руйнуванні водо-нафтової емульсії. Цей потік має регульовану витрату $F_{ne} = F_{ne}(t)$ та температуру $T_{ne} = T_{ne}(r, z, t)$.

Стійкість в часі водо-нафтової емульсії, яка надходить в термодегідратор — незначна. Тому можна вважати, що переважно в термодегідраторі перебуває двофазна система «знесолена нафта — промивна вода» з поверхнею розділу фаз, яка знаходиться на відстані r від його осі. Очевидним підходом при розробці ММ термодегідратора є складання рівнянь матеріального та енергетичного балансів саме для двофазної системи. В даному випадку ММ повинна буде містити рівняння динаміки для обох фаз: знесоленої сирової нафти та промивної води, що, безумовно, ускладнить диференціальну форму ММ та її подальшу чисельну реалізацію. Слушною альтернативою складанню системи рівнянь для двофазного потоку є відображення в ММ якісного переходу водо-нафтової емульсії в монофазні прошарки (знесолену сирину нафту та промивну воду). В якості ознак такого якісного переходу пропонується [2] розглянути швидкість $v(r, z, t)$ та температуру $\theta(r, z, t)$ реакції руйнування водо-нафтової емульсії. Тоді процес

відділення знесоленої сирі нафти від промивної води в термодегідраторі можна представити наступною ММ

$$\begin{aligned} \frac{\partial v(r, z, t)}{\partial t} = (r^2 - 1) \frac{\partial v(r, z, t)}{\partial z} + \frac{1}{r} \frac{\partial}{\partial r} \left[r \frac{\partial v(r, z, t)}{\partial r} \right] + \\ + \text{Pr}[1 - v(r, z, t)] \times \exp \left\{ \frac{v(r, z, t)}{1 + [v(r, z, t)/\gamma]} \right\}, \end{aligned} \quad (9)$$

$$\begin{aligned} \frac{\partial \theta(r, z, t)}{\partial t} = (r^2 - 1) \frac{\partial \theta(r, z, t)}{\partial z} + \frac{1}{r} \frac{\partial}{\partial r} \left[r \frac{\partial \theta(r, z, t)}{\partial r} \right] + \\ + k_o \text{Pr}[1 - \theta(r, z, t)] \times \exp \left\{ \frac{\theta(r, z, t)}{1 + [\theta(r, z, t)/\gamma]} \right\} \end{aligned} \quad (10)$$

з початковими

$$v(r, z, t)|_{t=0} = v_0, \quad \theta(r, z, t)|_{t=0} = \theta_0 \quad (11)$$

та граничними умовами

$$\begin{aligned} v(r, z, t)|_{r=1} = \zeta, \quad \theta(r, z, t)|_{r=1} = T_e(t), \quad v(r, z, t)|_{r=1} = \theta(r, z, t)|_{r=1} = 0, \\ \left. \frac{\partial v(r, z, t)}{\partial r} \right|_{r=0} = 0, \quad \left. \frac{\partial \theta(r, z, t)}{\partial r} \right|_{r=0} = \alpha_o [u(t) - \theta(r, z, t)], \quad \left. \frac{\partial v(r, z, t)}{\partial r} \right|_{r=1} = \left. \frac{\partial \theta(r, z, t)}{\partial r} \right|_{r=1} = 0, \end{aligned} \quad (12)$$

де $\text{Pr}[\cdot]$ — число Прандтля (враховує вплив фізичних властивостей теплоносія на тепловіддачу), k_o — термічний коефіцієнт впливу деемульгатора на температуру $\theta(r, z, t)$ реакції руйнування водо-нафтової емульсії, γ — питома вага однієї з фаз у двофазній системі (наприклад, знесоленої сирі нафти), α_o — коефіцієнт теплопередачі від шару деемульгатора, $u(t)$ — температура деемульгатора, ζ — деяка (у тривіальному випадку постійна) функція.

У рівняннях динаміки (9) та (10) експоненціальні члени відбивають монотонність перехідних процесів у термодегідраторі (тобто термодегідратор розглядається як аперіодична ланка 1-го порядку).

Як було зазначено вище, рівняння виду (9) — (12) задають ММ як термодегідратора, так і електродегідраторів в силу тотожності їх конструкції.

Апарати розсередженого теплообміну

Розсередженість цього класу апаратів зумовлено наявністю декількох поверхонь, на яких відбувається теплообмін. В даному випадку такими поверхнями є поверхні ректифікаційних (конденсаційних) тарілок колони попереднього відбензинювання, колони газової фракції та колони дизельної фракції. При розробці ММ апаратів розсередженого теплообміну для конкретності розглянемо колону попереднього відбензинювання.

Колона попереднього відбензинювання призначена для відділення з нафти розчинених газів та частини бензинової фракції і являє собою повну [3] колону, тобто має концентраційну (верхню) та кубову або відгінну (нижню) частини. Після

теплообмінників сумарним потоком $F_{33}(t)$ зневоднена та знесолена сира нафта при температурі $T_{33}(t)$ подається під нижню тарілку колони. З верху колони суміш вуглеводневого газу, парів води та бензину сумарним потоком $F_c(t)$ з температурою $T_c(r, z, t)$ надходить до конденсаторів-холодильників повітряного охолодження, після цього доохолоджується у водяному холодильнику, а далі ця газорідина суміш надходить до рефлексної ємності (останні три апарати детально не розглядаються, але при моделюванні їх класифіковано у відповідності до вище запропонованої класифікації).

Неконденсований газ з рефлексної ємності потоком $F_2(t)$ при температурі $T_2(t)$ спрямовується на блок амінової очистки (далі — не розглядається). Бензинова фракція з рефлексної ємності потоком $F_6(t)$ при температурі $T_6(t)$ подається в колону попереднього відбензинювання в якості гострого зрошення з корекцією температури $T_6(t)$ по температурі верху колони $T_6(r, z, t) = T_c(r, z, t)$. Відбензинена сира нафта з кубової частини колони попереднього відбензинювання у вигляді регульованого вихідного потоку $F_{66}(t)$ з температурою $T_{66}(r, z, t)$ відкачується до технологічних печей риформінгу бензину, де нагрівається і після цього надходить до атмосферної колони.

Рівень $h_k(r, z, t)$ в кубі колони попереднього відбензинювання підтримується з корекцією по витраті зневодненої та знесоленої сирової нафти $F_{33}(t)$ та витраті $F_{66}(t)$ відбензиненої нафти, що надходить до печей риформінгу бензину.

Поеднаємо в систему рівняння матеріального та енергетичного балансів для відгінної та концентраційної частин колони попереднього відбензинювання. В результаті отримаємо:

$$\left\{ \begin{array}{l} S_k \frac{\partial h_k(r_1, z, t)}{\partial t} = F_{33}(t) - F_c(t) - F_{66}(t); \\ \rho C_p S_k \left\{ \frac{\partial [h_k(r_1, z, t) T_{66}(r_1, z, t)]}{\partial t} \right\} = \rho C_p [F_{33}(t) T_{33}(t) - \\ - F_c(t) T_c(t) - F_{66}(t) T_{66}(r_1, z, t)]; \\ \frac{\partial T_c(r_i, z, t)}{\partial t} = v_{\text{зруш}} \left[\frac{\partial T_c(r_i, z, t)}{\partial r_i} - (r_i^2 - 1) \frac{\partial T_c(r_i, z, t)}{\partial z} \right] + \\ + (1/\xi_i) [T_6(t) - T_c(r_i, z, t)] - v_c \left[\frac{\partial T_c(r_i, z, t)}{\partial r_i} - (r_i^2 - 1) \frac{\partial T_c(r_i, z, t)}{\partial z} \right], \end{array} \right. \quad (13)$$

$$1/\xi_i = [(2\pi r_i \psi)/(\rho C_p S_k)], \quad i = 2, \dots, N$$

з початковими

$$\begin{aligned} F_{33}(t)|_{t=0} &= F_{33_0}, \quad F_{66}(t)|_{t=0} = F_{66_0}, \quad F_c(t)|_{t=0} = F_{c_0}, \\ T_{33}(t)|_{t=0} &= T_{33_0}, \quad T_{66}(r, z, t)|_{t=0} = T_{66_0}, \quad T_c(r, z, t)|_{t=0} = T_{c_0} \end{aligned} \quad (14)$$

та граничними умовами

$$\begin{aligned}
 h_k(r_1, z, t) \Big|_{r_1=0}^{r_1=r_{1\max}} = 0, \quad \frac{\partial h(r_1, z, t)}{\partial r} \Big|_{r_1=0}^{r_1=r_{1\max}} = 0, \quad h_k(r_1, z, t) \Big|_{z=z_k}^{z=z_{k\max}} = 0, \quad \frac{\partial h(r_1, z, t)}{\partial r} \Big|_{z=z_k}^{z=z_{k\max}} = 0, \\
 T_c(r_1, z, t) \Big|_{r_1=0}^{r_1=r_{1\max}} = T_{\text{вбн}}(t), \quad T_c(r_1, z, t) \Big|_{z=z_k}^{z=z_{k\max}} = T_{\text{зз}}(t), \\
 T_c(r_N, z, t) \Big|_{r_N=0}^{r_N=r_{N\max}} = T_{\text{б}}(t), \quad T_c(r_N, z, t) \Big|_{z=z_{\text{кн}}}^{z=z_{\text{кн}\max}} = T_{\text{с}}(t),
 \end{aligned} \tag{15}$$

де r_j — радіус ректифікаційних тарілок ($j=1, 2, \dots, N$; r_1 — радіус нижньої ректифікаційної тарілки), z_k — висота відгінної (кубової) частини колони попереднього відбензинювання, $z_{\text{кн}}$ — висота концентраційної частини колони попереднього відбензинювання, S_k — перетин відгінної (кубової) частини колони попереднього відбензинювання, ρ, C_p — відповідно густина та теплоємність нагрітої сирової нафти, ψ — коефіцієнт конвективного теплообміну між потоком зрошення та ректифікаційними тарілками, $v_{\text{зрш}}$ та v_c — відповідно швидкості зрошення та суміші вуглеводневого газу.

Система рівнянь (13) з початковими (14) та граничними (15) умовами (поширена відповідно на колони газової фракції та дизельної фракції) утворюють ММ апаратів розсередженого теплообміну.

Узагальнений математичний опис апаратів процесів первинної переробки сирих вуглеводнів

Аналізуючи ММ розглянутих апаратів процесів ППСВ визначимо можливості узагальненого математичного опису даних апаратів, що, у подальшому, дасть можливість уніфікувати на умовах типізації підходи до їх чисельної та обчислювальної реалізації.

В літературі, наприклад, [4 — 6], на основі законів Ньютона, Фур'є, Фіка та інших, виведено диференційні рівняння, які описують певні умови збереження маси та енергії, що пов'язані (рівняння) з дифузєю, теплопровідністю, тепломасопереносом, плином рідини, хімічними реакціями та іншими процесами. Зокрема в [6] було запропоновано узагальнений математичний опис даного класу процесів у вигляді диференційного рівняння в часткових похідних параболічного та гіперболічного типів. Однак це рівняння було виведено не на основі аналізу і узагальнення дифузійних та тепломасообмінних процесів, які відбуваються в реальних промислових об'єктах, а в результаті аналізу явищ, що відбуваються у деяких елементарних об'ємах гіпотетичних об'єктів. Ця обставина призводить до того, що запропонований математичний опис не може бути використаним в якості адекватної ММ процесів ППСВ, які розглянуто вище, оскільки зазначений опис має тільки методологічне значення.

Таким чином, використовуючи як основу для аналізу ММ процесів ППСВ, можна отримати, в якості їх узагальненого математичного опису, наступні рівняння у часткових похідних:

$$\begin{aligned}
 \frac{\partial \bar{\Phi}_i(r_j, z, t)}{\partial t} = f_i \left[\bar{\Phi}_i(r_j, z, t), \frac{\partial \bar{\Phi}_i(r_j, z, t)}{\partial z}, \frac{\partial^2 \bar{\Phi}_i(r_j, z, t)}{\partial r_j^2}, \frac{\partial \bar{\Phi}_i(r_j, z, t)}{\partial r_j}, \bar{U}_g(r_j, z, t) \right] + \\
 + D_i(\bar{\Phi}_i, r_j, z, t)
 \end{aligned} \tag{16}$$

$$\overline{\Phi} = [\Phi_1, \Phi_2, \dots, \Phi_k]^T \quad (T \text{ — знак транспонування})$$

з урахуванням початкових

$$\overline{\Phi}_i(r_j, z, 0) = \overline{\Phi}_{i_0}(r_j, z), \quad \forall i = 1, \dots, k; \quad \forall j = 1, \dots, N; \quad \forall (r_j, z) \in \Omega \quad (17)$$

та граничних умов наступних типів:

- граничних умов першого роду, ГУ-1 (типу Діріхле)

$$\overline{\Phi}_i(r_j, z, t) \Big|_{\substack{r_i=0 \\ r_i=r_{i\max} \\ z=0 \\ z=z_{\max}}} = \varphi_i[P_i(r_j, z, t)], \quad \forall i = 1, \dots, k; \quad \forall j = 1, \dots, N; \quad \forall (r_j, z) \in \Omega \quad (18)$$

- граничних умов третього роду, ГУ-3

$$\frac{\partial \overline{\Phi}_i(r_j, z, t)}{\partial r_i} \Big|_{\substack{r_i=0 \\ r_i=r_{i\max}}} = \lambda_i[\overline{\Phi}(r_j, z, t), P_i(r_j, z, t)], \quad (19)$$

$$\forall i = 1, \dots, k; \quad \forall j = 1, \dots, N; \quad \forall (r_j, z) \in \Omega,$$

де $\overline{\Phi}_i(r_j, z, t)$ — безперервні функції стану, що залежать від часової $t \in (0, t_k)$ та просторових $\forall (r_j, z) \in \Omega$ координат (координати r_j, z змінюються у відкритій (циліндричній) множині $\Omega \in R^{M_k}$ із гладкою границею $\partial\Omega$; R^{M_k} — евклідовий простір дійсних чисел розмірності M_k); функції стану $\overline{\Phi}_i(r_j, z, t)$ визначаються розв'язком системи (16) — (19), що (за визначенням) існує і є єдиним (нижче це посилання буде доведено); $\overline{U}_g(r_j, z, t)$, $g = 1, \dots, k^*$ — функції розподіленого управління, що належать гільбертовому простору $\overline{U}_{g_0}$ на R^{M_k} .

Змінні стану $\overline{\Phi}_i(r_j, z, t)$ та управління $\overline{U}_g(r_j, z, t)$ визначено у відкритих гільбертових просторах із границями відповідно $\Omega_{\Phi_i}, \Omega_{U_r}$, $\forall i = 1, \dots, k; \quad \forall r = 1, \dots, k^*$.

Функції $f_i[\cdot]$ та $y_i[\cdot]$ — безперервні лінійні або нелінійні функції; $D_i(\overline{\Phi}_i, r_j, z, t) = D_i\{r_j, z, t, \Phi_1(r_j, z, t), \Phi_2(r_j, z, t), \dots, \Phi_k(r_j, z, t)\}$ — лінійні або нелінійні функції, що характеризують дію зовнішніх збуджуючих впливів; $P_i(r_j, z, t)$, $\forall i = 1, \dots, k; \quad \forall j = 1, \dots, N; \quad \forall (r_j, z) \in \Omega$ — задані функції на границі $\partial\Omega$ області, які можуть виступати в якості граничних управляючих впливів; λ_i , $\forall i = 1, \dots, k$ — параметр, який характеризує енергетичні властивості елементів об'єкта (технологічного апарата); N — число поверхонь теплообміну (зокрема, ректифікаційних тарілок).

Змінні стану $\overline{\Phi}_i(r_j, z, t)$ та управління $\overline{U}_g(r_j, z, t)$ можуть визначати різні фізичні (зокрема, температуру, витрату), або геометричні (наприклад, рівень) величини, а також відхилення цих величин від стаціонарних значень; параметри λ_i визначають відповідно: коефіцієнт теплопровідності, коефіцієнт теплопередачі, тощо.

Отримані співвідношення (16) — (19) будемо вважати узагальненим математичним описом класу процесів ППСВ.

Висновки

Запропоновано ММ процесів ППСВ на прикладі технологічної схеми первинної переробки сирої нафти. Узагальнення та типізація цих ММ дозволяє при подальшій обчислювальній реалізації використовувати інструментарій у вигляді уніфікованого пакета прикладних модулів, побудованого на єдиній методологічній основі.

Список літератури

1. Технологический регламент установки ЭЛОУ—АВТ. ТР 00152282.006:2007. — Одесса: ОАО «ЛУКОЙЛ — Одесский НПЗ», 2007. — 208 с.
2. Погосов, А. Ю. Моделирование физических процессов и технологическая информатизация в нефтяной промышленности и энергетике: монография / А. Ю. Погосов, С. А. Положаенко, Ю. В. Григоренко. — Одесса: Наука и техника, 2013. — 656 с.
3. Каменских, И. А. Процессы и аппараты нефтяной и газовой промышленности / И. А. Каменских, В. А. Ведерников, В. А. Овчинникова. Учебник для ВУЗов. — Тюмень: ТюмГНГУ, 2002. — 192 с.
4. Патанкар, С. Численные методы решения задач теплообмена и динамики жидкости. — М.: Энергоиздат, 1984. — 152 с.
5. Козлов, Э. С. Автоматизация процессов решения краевых задач / Э. С. Козлов, Н. П. Сергеев, Н. С. Николаев. — М.: Энергия, 1984. — 112 с.
6. Егоров, А. И. Оптимальное управление тепловыми и диффузионными процессами. — М.: Наука, 1988. — 464 с.

МАТЕМАТИЧЕСКИЕ МОДЕЛИ И ОБОБЩЕНИЕ МАТЕМАТИЧЕСКОГО ОПИСАНИЯ ПРОЦЕССОВ ПЕРВИЧНОЙ ПЕРЕРАБОТКИ СЫРЫХ УГЛЕВОДОРОДОВ

Ю. В. Григоренко

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

Разработаны математические модели процессов и аппаратов первичной переработки сырых углеводородов, а также выполнено обобщение этих моделей с целью типизации и унификации математического описания класса процессов. Такого рода типизация дает возможность осуществить формализацию и унификацию методов и средств математического моделирования и, на этом основании, внедрить машинную реализацию указанных методов на единой унифицированной основе.

Ключевые слова: первичная переработка сырых углеводородов, математические модели, методы и средства математического моделирования

MATHEMATICAL MODELS AND GENERALIZATION OF MATHEMATICAL DEFINITION FOR PRIMARY PROCESSING OF CRUDE HYDROCARBONS

Yu. V. Grigorenko

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

Mathematical models for the processes and plants for primary processing of crude hydrocarbons were developed, and generalization of these models for typification and unification of mathematical definition of the process class was performed. Such typification enables to formalize and unify the methods and means of mathematical modeling, and, thereupon, to develop computerization of the specified methods using the unified basis.

Keywords: primary processing of crude hydrocarbons, mathematical models, methods and means of mathematical modeling.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 4, номер 2, 2014. Одеса – 95 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 4, номер 2, 2014. Одесса – 95 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 4, No. 2, 2014. Odesa – 95 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 №4 від 24.12.2013)

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

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

E-mail: immm.ukraine@gmail.com

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, 2014