МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 4, № 3

Volume 4, No. 3

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.

Published 4 times a year

Founded by Odessa National Polytechnic University in 2011

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

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

ЗМІСТ / CONTENTS

УДК 004.681.5

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 3, pp. 195-200

МОДЕЛІ ЗАГРОЗ ІНФОРМАЦІЙНОМУ ПРОСТОРУ СИСТЕМ УПРАВЛІННЯ ПОВІТРЯНИМ РУХОМ ТА МЕХАНІЗМИ ЙОГО ЗАХИСТУ

А.М. Орєхов, В.О. Хорошко

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

Розглянуто життєвий цикл інформації в системі управління повітряним рухом, яка знаходиться у інформаційному просторі, та вимоги до системи захисту. На їхній основі визначено перелік класів загроз та внутрішніх і зовнішніх зловмисників. З урахуванням дослідження створена модель загроз інформації.

Ключові слова: системи управління повітряним рухом, системи захисту інформації, інформаційний простір

Вступ

Сьогодні здійснюється перехід нашого суспільства від індустріального до інформаційного. Це стало можливим завдяки розвитку технологій, які дають змогу зберігати та обробляти великі масиви інформації, передавати її на великі відстані, здійснювати обмін цією інформацією між різними користувачами.

Перед Україною стала задача щодо входження до європейського та світового інформаційного простору для розширення взаємних зв'язків з різними державами. Тому питання захисту інформаційного простору та інформації, що передається, приймається та зберігається у ньому, є надзвичайно актуальними.

З урахуванням рівня втілення інформаційних технологій сучасності, розглядаючи інформацію як об'єкт діяльності, треба відзначити, що залежно від її важливості та значення для користування нею витрачаються відповідні ресурси. Але важливість та значення інформації для тих чи інших суб'єктів інформаційних відносин в умовах прихованого інтересу визначити складно. Тому зрозуміло, що задоволення інформаційних потреб перебуває в пропорційній залежності від умов та методів і засобів практичної діяльності відповідних суб'єктів, а високий рівень автоматизації, до якого прагне людство, ставить його в залежність від рівня безпеки інформаційних технологій, які воно використовує. Особливо це важливо для систем управління повітряним рухом (СУПР).

СУПР становить ключову складову національної аеронавігаційної системи України. На розвиток цієї системи відбиваються загальносвітові глобалізаційні тенденції, а саме відбувається інтенсивна інтеграція інформаційних активів систем на регіональному, національному та глобальному рівнях.

Інформаційний простір (ІП), що використовується зараз у СУПР, співпрацює за допомогою автономних локальних мереж. Проте, в перспективі завдяки розвитку глобального ІП інформаційні системи усіх участків процесу управління повітряним рухом інтегруватимуться в єдину систему, яка матиме відкриту розподілену архітектуру глобального масштабу.

Об'єднання ресурсів СУПР – це не самоціль, а за умов зростання попиту на авіаперевезення – це основа забезпечення потрібного рівня безпеки польотів, підвищення пропускної спроможності та економічної ефективності авіаційної галузі.

Авіаційна спільнота вже звернула увагу на той факт, що ІП і мережі, які використовуються СУПР, є потенційно вразливими при втручанні віддалених хакерів та інсайдерів. Експерти з питань інформаційної безпеки виявляють значну кількість «шпарин» у них, неспроможність авіаційних адміністрацій виявити вторгнення і підтримувати працездатність системи у разі порушення захисту через неадекватне управління ІП, оновленням програмного забезпечення, обліковими записами, паролями і привілеями користувачів, а також через ігнорування потреби у відслідкуванні причин подій, що стосуються безпеки.

Основна частина

Будь-яку інформацію розглядають у вигляді потоків, які діють на органи сприйняття користувача формами зображення, звуку та тексту, що призводять до породження потоків відповідних форм.

Визначення 1. Інформація – такий стан суспільно - політичних та соціально – економічних відносин у державі (групи держав), за якого реальні важелі впливу на формування і введення державної зовнішньої і внутрішньої політики мають особи (угрупування), що ініціюють та/або контролюють основні процеси та/або явища в інформаційному середовищі, а також розподіляють інформаційні потоки у зазначеній державі (групи держав).

Визначення 2. Інформаційний потік - рух інформації в ІП.

Сучасні інформаційні технології сублімують у собі якості усіх форм, різні поточні форми можуть трансформуватися між собою. Умовно всі трансформації в СУПР визначено як трансформації інформаційних потоків, модифікація яких ставить питання порушення цілісності та достовірності інформації (властивості інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом). Інформаційні потоки поділяють на елементарні структурні одиниці – файли чи повідомлення.

Визначення 3. Файл – це іменована область пам'яті системи, яка містить компоненти одного типу.

Наукова проблема цілісності інформації, яка сформульована у межах цієї статті - це цілісність окремого файлу наданого формату.

Розглядання інформаційних трансформацій на предмет реалізації поставлених вимог диктує необхідність локалізації її основних процесів.

Оскільки ми орієнтуємось на захист відомчих інтересів, тобто СУПР, треба зауважити, що на всіх етапах [1, 2] трансформації інформації (відомостей) визначається деякий проміжок часу, тобто інформація має певний життєвий цикл (див. рис.1).

Життєвий цикл інформації у ІП СУПР залежить від оцінки її цінності, а також відповідно від спроможності санкціонованих користувачів забезпечити її надійний захист, і, отже, не допустити «знецінення» та «знищення» інформації. Він передбачає, що інформація здобувається, обробляється (анімується), зберігається, охороняється, використовується, транслюється та знищується. Тому розглянемо етапи життєвого циклу інформації з позиції цільової ознаки системи контролю цілісності та достовірності інформації (СКЦДІ) детальніше, щоб відокремити вразливі ланки трансформації, які потребують захисту. Підкреслимо, що модифікації інформації охоплює всі етапи життєвого циклу. Під терміном «модифікація» будемо розуміти будь-яку зміну попереднього змісту інформації стосовно етапу її створення (див.рис.1).

Процеси створення та знищення інформації, тобто відображення або створення на матеріальному носії: електронної накопиченої інформації з урахуванням визначених

завдань користувачами. Після отримання і створення інформаційного масиву здійсняється його оцінка на предмет відповідності абстрактним і конкретним вимогам щодо подальшого використання у визначених (дозволених) межах. Зберігання вимагає розроблення порядку та правил підготовки до зберігання інформації в електронному вигляді з технологією обмеження доступу. Вибірка інформації та подальша оцінка вибору зумовлена конкретністю поставленої задачі. Критичність щодо інформації постає з моменту вибірки та подальшого такого опрацювання.

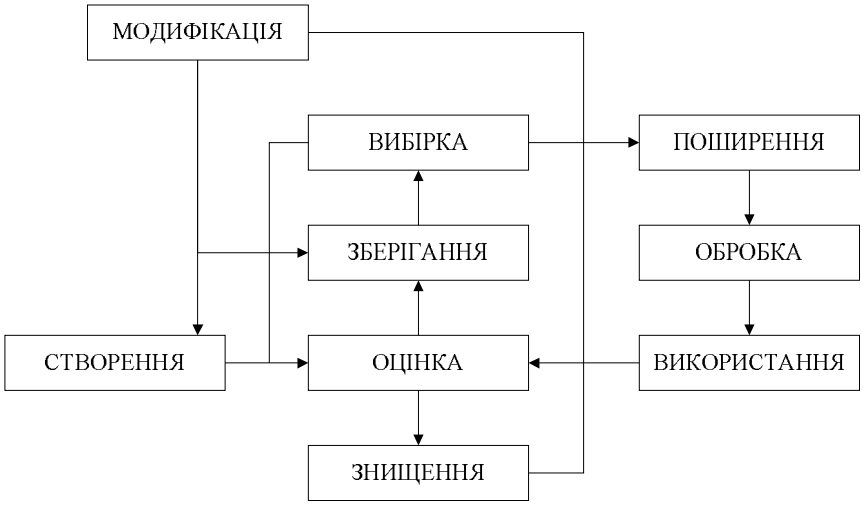


Рис. 1. Життєвий цикл інформації у ІП СУПР

Обробка та використання інформації суб'єктами ІП СУПР, які зумовлюють практичне використання інформації у своїй роботі при прийнятті рішень та реалізації тих чи інших процесів у керуванні повітряним простором, дає змогу виділити найуразливішу ланку захищеного ІП – етап передавання інформації, де є можливість несанкціонованих дій зловмисника або неавторизованого користувача (перегляду, модифікації, знищення).

Засоби контролю цілісності та достовірності інформації функціонують на різних структурних рівнях її обробки. Це низький, середній та високий: низький (структурний рівень), середній (семантичний рівень подання інформації) та високий (логічний рівень контексту інформації) рівні. Розглядання високого рівня виходить за межі цієї статті, засоби середнього рівня аналізується у цій роботі.

На низькому (структурному) рівні обробки інформації автоматизованим робочим місцем [2, 3] функціонують методи, які відповідають СКЦДІ.

Отже, вирішення проблеми цілісності та достовірності інформації зумовлює розгляд елементів його сигнатурного аналізу та побудови функцій хешування даних, які формулюються з урахуванням та систематизації переліку загроз інформації та класифікації характеристик файлу ІП, які критичні до модифікування.

Обробка інформації пов'язана з формою подання на подразники остаточної інформації (текст, зображення, звук). Крім перелічених інформаційних потоків, існують ще деякі службові дані, що характеризують програмне середовище та відображають його функціональність (відповідність призначенню). Тобто інформаційний потік залежно від сприйняття поданій в формі текстового, графічного або звукового потоку, потоку відео зображення та службового потоку, який циркулює на рівні функціонування вузлів обробки інформації, СУПР та забезпечує існування перерахованих потоків в сучасному ІП управління повітряним простором.

На низкому рівні інформаційні потоки – це послідовність байтів стандартного оформлення (формати даних). Під модифікацією файлів розуміється модифікація потоків, оскільки перший є структурною одиницею потоку.

Визначення 4. Загроза інформаційної безпеки ІП СУПР – це можливість реалізації впливу на інформацію у ІП, що призводить до створення, знищення, блокування доступу до інформації, також можливість впливу на компоненти СУПР, що призводить до втрат, знищення або збою функціонування системи, засобів взаємодії з постачальником інформації або засобів управління системою та ІП.

Необхідність класифікації загроз інформаційній безпеці зумовлена тим, що архітектура сучасних засобів автоматизованої обробки, організаційна структурна та функціональна побудова СУПР та їх мереж, технології та умови обробки такі, що інформація потрапляє під вплив надмірної кількості чинників, за якими і потрібно формалізувати задачу описання загроз та ефективної протидії їм. Перелік загроз інформаційної безпеки [3] будемо розглядати за цільовою ознакою класифікації та описання складних інформаційних потоків, критичних до модифікування та впливів. Аналіз цих загроз повинен бути здійснений на основі їхньої класифікації за низкою ознак [4]. Кожне з цих ознак відображає одну із узагальнених вимог до системи захисту (конфіденційність, цілісність, достовірність): необхідність дії, що призводить до можливості несанкціонованого доступу до конфіденційної інформації або роблять її загальнодоступною; ігнорування організаційних обмежень (встановлених правил) під час визначення рангу системи; несанкціоноване втручання в роботу ІП або модифікування інформації, що впливає на штатну роботу СУПР.

Для системи визначимо перелік класів загроз (якості моделі): за природою виникнення; за ступенем навмисності; за безпосереднім джерелом загроз; за станом джерел загроз; за мірою залежності від активності СУПР; за мірою впливу на СУПР та ІП; за станом доступу користувачів або програм до ресурсів ІП СУПР; за способом доступу до ресурсів ІП СУПР; за поточним місцем розміщення інформації, що зберігається і обробляється в СУПР.

Відповідно для ІП та СУПР будемо розглядати наступні види загроз: порушення конфіденційності (інформація стає відома тим, хто не повинен нею володіти); порушення цілісності (включає в себе поняття будь-якої навмисної зміни інформації, що зберігається або обробляється в СУПР або при її передаванні між елементами системи; розкриття параметрів СУПР.

Розглядаючи питання захисту ІП та СУПР, доцільно використовувати чотирирівневу градацію доступу до інформації, що зберігається, обробляється та залишається в ІП та СУПР: рівень інформаційних ресурсів; рівень засобів взаємодії з інформаційними ресурсами; рівень надання інформації; рівень захисту інформації.

Потрібно сформулювати додаткові вимоги щодо аналізу загроз інформації:

- перелік загроз повинен бути максимально повним та деталізованим. Для кожної із загроз необхідно визначити, на порушення яких властивостей інформації або СУПР вона спрямована (конфіденційності, цілісності, доступності, а також відмови служб СУПР);
- можливі методи реалізації загроз [5].

З урахуванням технології обробки інформації та побудови моделі загроз інформації необхідно розробити модель зловмисника, яка повинна бути адекватна реальному зловмиснику для певної СУПР.

Визначення 5. Модель зловмисника – абстрактне формалізоване або неформалізоване описання дій зловмисника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце тощо.

Стосовно СУПР зловмисники можуть бути зовнішніми або внутрішніми. Модель зловмисника повинна визначати: можливу мету зловмисника та її градацію за ступенем

небезпеки для СУПР; категорії осіб, із яких може бути зловмисник; передбачення про кваліфікацію зловмисника; передбачення про характер дій зловмисника.

Метою зловмисника може бути можливість вносити зміни в інформаційні потоки згідно зі своїми намірами та завдання завдати збитків через знищення інформації.

Будь-яка якісна система протидії апріорно передбачає високий досвід та кваліфікацію зловмисника (можливість використання недоліків проектування комплексної системи захисту СУПР за допомогою методів та засобів активного впливу на СУПР, які змінюють конфігурацію системи).

Також передбачається, що за місце дій зловмисники можуть одержати доступ до засобів адміністрування СУПР та засобів управління комплексною системою захисту.

Перелік загроз [4, 5], оцінка їхньої реалізації, модель зловмисника є основою для аналізу ризику реалізації загроз та формулювання рис моделі реєстрації даних.

Дія моделі реєстрації даних поширюється на рівень аутентифікації файлів.

Перша умова функціонування моделі – автономність СКЦДІ (незалежність від дій системного адміністрування). Умова друга – обов'язковість (застосування алгоритмів СКЦДІ до кожного елемента потоку). Умова третя – компактність засобів СКЦДІ (застосування мінімальних обчислювальних ресурсів). Умова четверта - реагування (комплекс організаційних заходів щодо порушення цілісності об'єкта).

Враховуючи, що файл є одиницею між різними системами обробки інформації і він виступає як індикатор СКЦДІ, розглядаємо характеристики файлу як одиниці, до якої можливе застосування моделі реєстрації та підтвердження їхньої цілісності.

Створення механізму ефективного захисту інформації з обмеженням доступом передбачає, насамперед, уявлення, що в основі існує стандартна система, яка складається з об'єкта нападу (ІП СУПР та сам СУПР) та суб'єкта, який намагається використати інформацію всупереч встановленим нормам поводження з нею.

Проаналізувавши життєвий цикл інформації в СУПР, визначимо питання щодо його аналізу: як транспортувати інформацію; який вид аналізу застосувати для визначення стану інформації після її транспортування?

Якщо позначка дослідження – вибір виду аналізу, то об'єктом аналізу, зважаючи на це, стає структурування інформації у ІП.

Сформулюємо тезисно відповіді на ці два питання, які були поставлені. Інформаційний потік, що контролюється, переважно передаватиметься у відкритому вигляді (для безпосереднього подальшого опрацювання) з подальшою обов'язковою обробкою СКЦДІ у СУПР.

За наявності такого функціонуючого механізму, у разі нападу на передачу інформацію своєчасне виявлення цього факту надасть додаткові можливості щодо запобігання подальшому розвитку негативних подій.

Висновки

На основі проведеного дослідження можна зробити такі висновки. Розгляд особливостей функціонування існування інформації в електронному вигляді дає змогу виділити такі риси інформаційної моделі реєстрації даних у ІП СУПР.

Трансляція інформації в мережах телекомунікацій відбувається у вигляді інформаційних потоків, класифікація яких залежить від сприйняття їх оператором (текстові, графічні, відео та службові потоки: кодування архівація, стиснення) та характеризується внутрішньою структурою формату потоку. Елементарною структурною одиницею потоку є файл, який будується з однотонних даних.

Інформація в сучасних СУПР часто може піддаватися несанкціонованій модифікації (прояви тероризму). Найуразливішим із основних етапів життєвого циклу інформації є її поширення між операторами (користувачами) у ІП.

Розглядаючи питання захисту ІП СУПР та самої системи, доцільно використовувати чотирирівневу градацію доступу до інформації, що зберігається, обробляється та захищається у СУПР.

Стосовно інформації необхідно виділити методи реалізації загроз на кожному рівні. Характеристика потенційних зловмисників припускає їхніх високий досвід та кваліфікацію, а також передбачається, що за місцем здійснення дій зловмисника можуть одержати доступ до засобів адміністрування СУПР та засобів управління комплексною системою захисту.

Дія моделі реєстрації даних поширюється на рівень аутентифікації файлів. Виділені критичні параметри файлу, що схильні до модифікації. Це як зовнішні, так і внутрішні файли.

Визначені умови функціонування моделі реєстрації даних, які поширюються на рівень аутентифікації файлів.

Список літератури

1. Ленков, С.В. Методы и средства защиты информации в 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А.-К.: Арий, 2008.
2. Бурячок, В.Л. Політика інформаційної безпеки / Бурячок В.Л., Грищук Р.В., Хорошко В.О.-К.: ПВП «Задруга», 2014.-222с.
3. Кобозева, А.А. Аналіз захищеності інформаційних систем / Кобозева А.А., Мачалін І.О., Хорошко В.О.-К.: Вид ДУІКТ, 2010.-316С.
4. Иванченко, Е.В. Модель и метод оценки эффективности организации процесса функционирования систем воздушного движения / Иванченко Е.В., Орехов А.Н., Хорошко В.А. // Сучасний захист інформації, Спец. Випуск, 2013.-с. 73-81.
5. Капустян, М.В. Оценка эффективности функционирования сложных систем / Капустян М.В., Хорошко В.А. // Інформаційна безпека, №1, 2011.-с. 5-8.

МОДЕЛИ УГРОЗ ИНФОРМАЦИОННОМУ ПРОСТРАНСТВУ СУВД И МЕХАНИЗМЫ ЕГО ЗАЩИТЫ

А.М. Орехов, В.А. Хорошко

Национальный авиационный университет,
пр. Космонавта Комарова, 1, Киев, 03058, Украина; e-mail: professor_va@ukr.net

Рассмотрен жизненный цикл информации в системе управления воздушным движением, которая находится в информационном пространстве и требования к системе защиты. На их основе определен перечень классов угроз и внутренних и внешних злоумышленников. С учетом исследования создания модель угроз информации.

Ключевые слова: системы управления воздушным движением, системы защиты информации, информационное пространство

AIR-TRAFFIC CONTROL SYSTEM CYBERSPACE: MODELS OF THREATS AND PROTECTION MECHANISMS

A.M. Orehov, V.O. Khoroshko

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

Lifecycle of air-traffic control system information related to cyberspace, as well as requirements to the protection system were discussed. On this basis, a list of classes of both the threats and external and internal intruders was identified and a model for cyberspace threats was developed.

Keywords: air-traffic control system, information protection systems, cyberspace

УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 3, pp. 201-209

ПРАКТИЧЕСКОЕ ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ СИСТЕМ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

В.А. Болтенков, Р.И. Еникеев

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

Исследованы современные алгоритмы электронной цифровой подписи (ЭЦП). Алгоритмы проанализированы с точки зрения удобства программной реализации и быстродействия на различных этапах ЭЦП. Исследованы наиболее применяемые криптографические хэш-функции как составная часть системы ЭЦП. Исследование проведено путем программной реализации различных систем ЭЦП на языке Java с использованием библиотеки Open SSL и последующим программным профилированием.

Ключевые слова: электронная цифровая подпись, хэш-функция, стандарты цифровой подписи, асимметричные криптографические системы, быстродействие

Введение

Электронная цифровая подпись (ЭЦП) (англ. digital signature) за почти сорокалетнюю историю своего существования прошла стремительную эволюцию от математической идеи У. Диффи и М. Хеллмана, высказанной в 1976 г. [1], до неотъемлемого элемента современного защищенного сетевого электронного документооборота. ЭЦП – реквизит электронного документа, предназначенный для защиты электронного документа от подделки или внесения изменений, полученный в результате криптографического преобразования информации с использованием секретного ключа подписи и позволяющий идентифицировать владельца ключа подписи и установить отсутствие искажения информации в электронном документе. ЭЦП также обеспечивает невозможность отказа лица, подписавшего документ от его акта подписания. Благодаря этим свойствам ЭЦП широко применяется в следующих сферах:

- безопасный банковский финансовый оборот,
- юридически значимый электронный документооборот,
- юридическая и финансовая обязательная отчетность перед государственными органами,
- таможенное декларирование товаров и услуг,
- расчетные и трейдинговые системы,
- дистанционные торговые сделки.

Несмотря на повсеместное использование ЭЦП в перечисленных сферах применения, на сегодняшний день сложилась достаточно парадоксальная ситуация – параллельно существуют и применяются различные государственные и коммерческие стандарты ЭЦП, при этом пользователь системы ЭЦП обычно плохо представляет себе эффективность и качество применяемой им системы, ее степень криптостойкости и может реально оценить только удобство интерфейса программной реализации ЭЦП и ее быстродействие. Следует отметить, что многие из применяемых систем ЭЦП основаны на вычислительно трудоемких алгоритмах, что вызывает ощутимые пользователем временные задержки и вызывает неудовлетворенность применяемой им

системой. Несмотря на обилие публикаций по криптографическим протоколам, к которым относится и ЭЦП [2,3], авторам неизвестен обстоятельный сравнительный анализ существующих и применяемых систем ЭЦП. В этом плане задача сравнительного исследования различных алгоритмов и систем ЭЦП по набору критериев эффективности является достаточно актуальной.

Практически все протоколы ЭЦП используют криптографические хэш-функции, позволяющие путем применения математического сжимающего преобразования получить из документального файла произвольного размера результат фиксированной длины – дайджест сообщения. В целях уменьшения вычислительного объема ЭЦП и снижения времени на ее формирование и проверку алгоритмы формирования ЭЦП применяются к дайджестам, которые существенно короче исходных сообщений. В этом плане качество системы ЭЦП в значительной мере определяется применяемым алгоритмом хэш-функции. Поэтому сравнительный анализ систем ЭЦП обязательно должен сопровождаться исследованием показателей эффективности применяемых хэш-функций [4].

Целью настоящего исследования является сравнительный анализ наиболее популярных систем ЭЦП, включая исследование применяемых хэш-функций, путем их программной реализации с последующим тестированием и профилированием.

Критериями для сравнения систем были выбраны: удобство программной реализации системы ЭЦП и время ее работы, которое как указано выше, напрямую связано с удобством пользователя. Под удобством программной реализации будем понимать:

- наличие открытого исходного кода,
- наличие криптопримитивов данной системы ЭЦП в открытых библиотеках программных кодов,
- возможность распараллеливания алгоритма и наличие других путей ускорения действия алгоритма при его программной реализации.

Криптостойкость ЭЦП как и всех криптографических протоколов с открытым ключом не имеет теоретического обоснования, поэтому в данном вопросе мы ориентировались на концепцию «практической границы уровня безопасности в 80 бит длины ключа», согласно которой асимметричная криптосистема с длиной ключа 80 бит и более не может быть взломана атакой грубой силы за разумное время [5], а также соответствующими стандартами ЭЦП.

Под временем работы алгоритма электронной подписи будем понимать сумму затрат времени на операции «генерация ключа подписи», «постановка подписи», «верификация подписи». Время работы зависит от скоростных качеств криптоалгоритма, реализующего цифровую подпись и скорости применяемой хэш-функции.

В силу существенной нелинейности как алгоритмов криптографического хэширования, так и алгоритмов ЭЦП, не представляется возможным получить хотя бы грубые оценки вычислительной сложности систем ЭЦП. Поэтому основным методом их сравнительного анализа была выбрана программная реализация различных систем ЭЦП с последующим их тестированием и профилированием.

Основная часть

Общая схема ЭЦП. Независимо от применяемого алгоритма общая схема ЭЦП в системе асимметричного шифрования может быть представлена следующим образом [3]. На первом шаге вычисляется хэш-функция h от передаваемого документа (сообщения) M и создается дайджест документа $m = h(M)$. При помощи секретного ключа отправителя A k_A и алгоритма формирования ЭЦП E создается

зашифрованный дайджест сообщения M $C(m)$. В пакет для получателя B включаются: сообщение M, ЭЦП $C(m)$ и открытый ключ отправителя K_A, пакет передается получателю B по открытому каналу связи (отметим, что открытый ключ K_A может не передаваться по каналу связи, а публиковаться каким-либо другим образом, например, размещаться на сайте) (рис.1). На этапе верификации подписи получатель B вычисляет хэш-функцию $h(M)$ и получает дайджест m', расшифровывает ЭЦП алгоритмом дешифрования D, получает при этом дайджест m'. Далее производится сравнение двух хэш-функций m' и m. Их совпадение гарантирует одновременно подлинность содержимого документа и его авторства, в случае несовпадения подпись отвергается (рис.2).

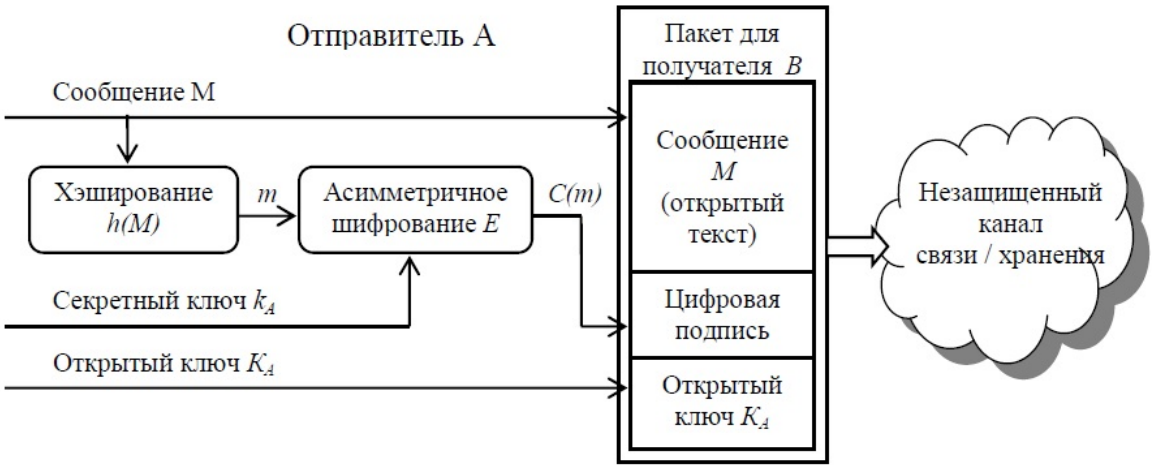


Рис.1. Общая схема ЭЦП (этап формирования)

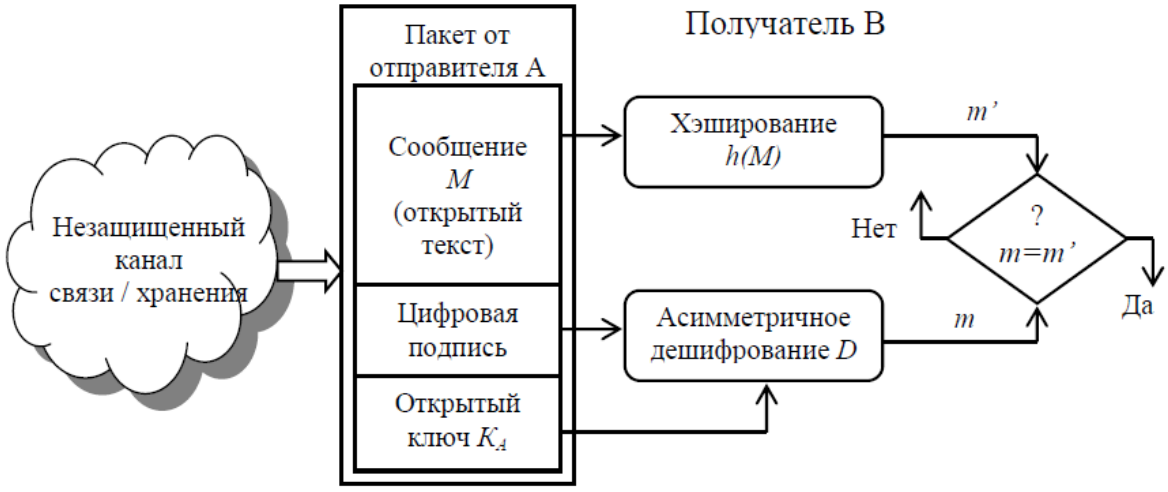


Рис.2. Общая схема ЭЦП (этап верификации)

Алгоритмы ЭЦП. Кратко рассмотрим современные алгоритмы ЭЦП, применяемые на практике. Все они основаны являются асимметричными, т.е. применяют открытый ключ. По типу применяемой односторонней функции с лазейкой (one-way function with trapdoor) они делятся на системы основанные на:

- факторизации произведения двух больших простых чисел,
- вычислении дискретного логарифма в конечном поле,
- задаче дискретного логарифмирования на эллиптических кривых в конечном поле.

Алгоритм RSA (аббревиатура от фамилий создателей Rivest, Shamir и Adleman) – первый практический криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Был создан в Массачусетском технологическом институте (MIT) в 1977 г. Защищен патентом США 4405829, выданным 20 сентября 1983 г. и действующим с продлениями до сих пор. В 1982 году Ривест, Шамир и Адлеман организовали компанию RSA Data Security, являющуюся единственным владельцем и распространителем алгоритма. На сегодняшний день RSA является фактически неофициальным мировым коммерческим стандартом ЭЦП, это самый применяемый в мире алгоритм подписи, по некоторым экспертным оценкам им подписывается до 90% всех документов. Однако главным недостатком RSA является его закрытый код и необходимость приобретения лицензии.

Алгоритм DSA (Digital Signature Algorithm) разработан Национальным институтом стандартов и технологий США (НИСТ) в августе 1991г. и защищен патентом США 5 231 668, однако НИСТ сделал этот патент доступным для использования без лицензионных отчислений. Поскольку алгоритм стал свободным для использования, его можно свободно реализовывать программным, аппаратным или любым другим образом. Основан на сложности задачи дискретного логарифмирования. Алгоритм вместе с криптографической хеш-функцией SHA-1 является частью стандарта США DSS (Digital Signature Standard), впервые опубликованного в 1994 г.

Остальные рассмотренные алгоритмы основаны на эллиптической криптографии – разделе криптографии, который изучает асимметричные криптосистемы, основанные на эллиптических кривых над конечными полями. Основное преимущество эллиптической криптографии заключается в том, что на сегодняшний день неизвестно существование субэкспоненциальных алгоритмов решения задачи дискретного логарифмирования.

Алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm) – алгоритм с открытым ключом для создания цифровой подписи, аналогичный, по своему строению, DSA, но определённый, в отличие от него, не над полем целых чисел, а в группе точек эллиптической кривой. ECDSA является очень привлекательным алгоритмом для реализации ЭЦП. Самым важным преимуществом ECDSA является возможность его работы на значительно меньших конечных полях. Как, и вообще в криптографии на эллиптических кривых, предполагается, что битовый размер открытого ключа, который будет необходим для ECDSA, равен двойному размеру секретного ключа в битах. Для сравнения, при обеспечении уровня безопасности в 80 бит (т.е. когда атакующему полным перебором необходимо рассмотреть примерно 2^{80} версий подписи для нахождения секретного ключа), размер открытого ключа DSA равен, по крайней мере, 1024 бит, тогда как открытого ключа ECDSA – 160 бит. С другой стороны размер подписи одинаков и для DSA, и для ECDSA: $4t$ бит, где t – уровень безопасности, измеренный в битах, то есть – примерно 320 бит для обеспечения уровня безопасности в 80 бит. Иными словами, любая криптосистема на эллиптической кривой обеспечивает ту же криптостойкость, что и система, основанная на дискретном логарифмировании при существенно меньшей длине ключа.

Алгоритм ГОСТ Р34.10-2012 – российский стандарт, описывающий алгоритмы формирования и проверки электронной цифровой подписи. Принят и введён в действие в 2012 г.

ДСТУ 4145-2002 (полное название: «ДСТУ 4145-2002. Информационные технологии. Криптографическая защита информации. Цифровая подпись, основанная

на эллиптических кривых. Формирование и проверка») – украинский стандарт, описывающий алгоритмы формирования и проверки электронной цифровой подписи [6]. Принят и введён в действие в 2002 г. Несмотря на достаточно долгое существование ДСТУ 4145-2002 в качестве государственного стандарта ЭЦП, он остается декларированным, но мало применимым, несмотря на то, что его основные криптопримитивы реализованы в открытых Java-библиотеках OpenSSL и Bouncy Castle. По нашему мнению, существует две причины этого:

- очень сложное изложение текста самого стандарта; хотя официальное издание [6] содержит всего 39 страниц, чтение документа и его понимание занимает длительное время даже у достаточно подготовленных профессиональных программистов,
- практически полное отсутствие возможностей распараллеливания при программной реализации алгоритма.

Результаты предварительного анализа всех перечисленных алгоритмов сведены в таблицу 1.

Таблица 1.

Основные характеристики алгоритмов ЭЦП

Алгоритм	Хэш-функция	Рекомендованный размер открытого ключа	Рекомендованный размер закрытого ключа	Год создания, страна
DSA	SHA1 или SHA2	1024-3072 бит	160-256 бит	1994, США
ECDSA	SHA1 или SHA2	112-320 бит	80-521 бит	1999, США
ГОСТ Р 34.10-2012	ГОСТ Р34.112012	80-320 бит	256-512 бит	2012, РФ
ДСТУ 4145-2002	ГОСТ 34.311	162-768 бит	256-1024 бит	2002, Украина

Не останавливаясь детально на обзоре применяемых в ЭЦП критографических хэш-функций, скажем только, что все они основаны на алгоритмах блочного шифрования. В данном исследовании ЭЦП были применены хэш-функции MD-2 MD-5 SHA-1 SHA-2 (с размерами блока 256, 384, 512 бит), также ГОСТ 34311.95 и ГОСТ Р34.112012, специфицированные соответствующими стандартами ЭЦП [2,3] .

Программное средство для моделирования и сравнительного анализа систем ЭЦП

Для сравнительного анализа систем ЭЦП путем моделирования разработано универсальное программное средство со следующими функциями:

- блок хэширования,
- блок генерации открытого ключа,
- блок генерации секретного ключа,
- блок формирования ЭЦП,
- блок верификации ЭЦП.

Программа разработана на языке Java с применением библиотеки криптопримитивов Open SSL. Open SSL (secure socket layer - система безопасных сокетов) – криптографический пакет с открытым исходным кодом, предоставляющий богатые средства для профилирования программных фрагментов по затратам процессорного времени [7]. На рис.3 приведена основная экранная форма программы.

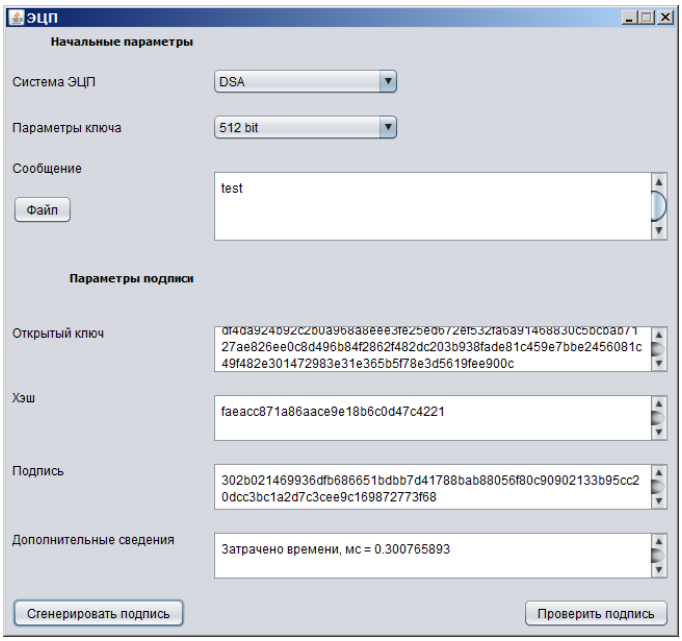


Рис.3. Основная экранная форма программы моделирования ЭЦП

Результаты исследований

Моделирование ЭЦП в целом и хэш-функций проводилось на аппаратно-программных конфигурациях двух типов:

- конфигурация А:
  CPU: Pentium 987(ядро Sandy Bridge) 1.5 ГГц (2 МБ L1 cache);
  RAM: 4 ГБ DDR3 1300 МГц;
  ОС: Win7,
- конфигурация Б:
  CPU: Core i5 3240T(ядро Ivy Bridge) 2.9 ГГц (3 МБ L1 cache);
  RAM: 8 ГБ DDR3 1600 МГц;
  ОС: Win7.

Конфигурация А моделирует типичный современный офисный компьютер в организациях и компаниях, применяющих ЭЦП, а конфигурация Б - типичный компьютер, применяемый в подразделениях компьютерной безопасности банков и других финансовых учреждений, верифицирующих ЭЦП.

В процессе моделирования была исследована производительность (скорость работы) хэш-функций. Усредненные по базе файлов документов различных форматов и размеров объемом $3 \cdot 10^4$ файлов результаты исследования быстродействия хэш-функций приведены в таблице 2 и на рис.4. Показатели скорости оценены программными профилировщиками, а также программными средствами Java и Open SSL.

Видно, что хэширование с помощью SHA-2 с длиной блока 512 бит является наиболее производительной вычислительной процедурой. С другой стороны, алгоритм SHA-2 является достаточно современной и перспективной функцией хэширования, что гарантирует ее криптостойкость.

Таблица 2.

Результаты исследования быстродействия хэш-фукций

Функция хэширования	Количество раундов	Язык реализации	Скорость работы на конфигурации А, Мбит/с	Скорость работы на конфигурации Б, Мбит/с
SHA-1	80	Java	206	344
SHA-2(256)	64	Java	81	135
SHA-2(512)	64	Java	41	68
ГОСТ 34311.95	256	Java	49	83
ГОСТ Р34.112012	256	Java	28	46

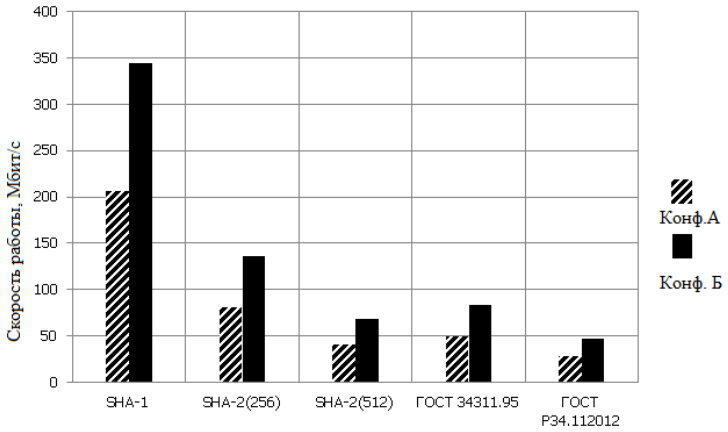
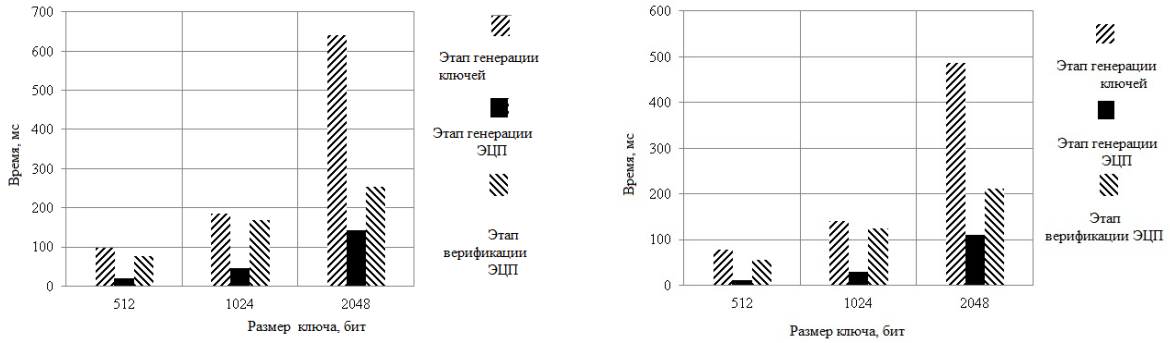


Рис. 4. Сравнительный анализ скорости работы хэш-функций

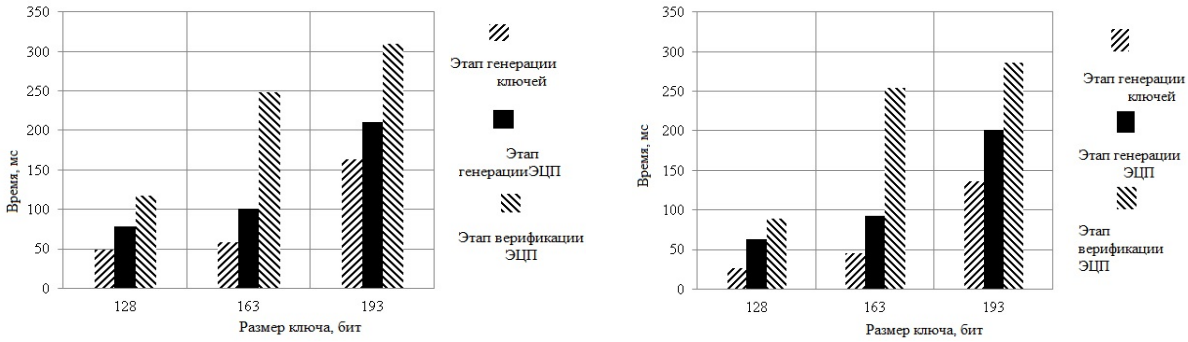
При исследовании алгоритмов ЭЦП был проведен предварительный анализ систем ЭЦП, приведенных выше в таблице 1. Он позволил вывести мягкую рейтинговую оценку, согласно которой программная реализация алгоритмов ГОСТ Р 34.10-2012 и ДСТУ 4145-2002 существенно сложнее алгоритмов DSA и ECDSA, поэтому при требуемых длинах ключей ГОСТ Р 34.10-2012 и ДСТУ 4145-2002 практически не выдерживают конкуренции с алгоритмами DSA и ECDSA по быстродействию. Ниже приведены результаты анализа быстродействия только для наиболее быстрых систем ЭЦП DSA и ECDSA.

Оценка быстродействия систем ЭЦП DSA и ECDSA, в зависимости от длины ключа с разбивкой по этапам, представлены на рис. 5-6 для обеих аппаратных конфигураций.



а **б**

Рис. 5. Временной анализ этапов ЭЦП DSA в зависимости от размера ключа: а – конфигурация А; б – конфигурация Б



а **б**

Рис. 6. Временной анализ этапов ЭЦП ECDSA в зависимости от размера ключа: а – конфигурация А; б – конфигурация Б

Анализ графических зависимостей позволяет установить следующие интересные факты.

Подпись на эллиптических кривых требует существенно большего времени на верификацию, чем на формирование ключей.

Для пользовательской конфигурации А вполне приемлемо с точки зрения быстродействия для системы DSA рекомендовать длину ключа 1024 бита, а для системы ECDSA - длину ключа 163 бита. Для профессиональной конфигурации Б эти рекомендации сохраняются.

Общие рекомендации, полученные в результате исследования, сформулируем таким образом. Наиболее эффективными по формулированным критериям удобства программной реализации и быстродействия являются системы ЭЦП DSA и ECDSA с применением хэш-функции SHA-2 длиной блока 256 или 512 бит. При сравнении систем DSA и ECDSA последнюю, безусловно, следует считать более перспективной, поскольку большинство действующих стандартов ЭЦП ориентированы на эллиптическую криптографию.

Выводы

Исследование современных систем ЭЦП путем их программного моделирования по критериям удобства программной реализации и быстродействия позволило

установить, что системы DSA и ECDSA в сочетании с хэш-функцией SHA-2 в наибольшей мере удовлетворяют сформулированным критериям и могут быть рекомендованы для практического применения. Выработаны практические рекомендации по длине блоков хэш-функции и длине ключа алгоритмов ЭЦП.

Список литературы

1. Diffie, W. New Directions in Cryptography / W. Diffie, M. Hellman. // IEEE Transactions on Information Theory. –Vol.22. No.6, 1976. – pp. 644–654.
2. Черемушкин, А.В. Криптографические протоколы. Основные свойства и уязвимости. – М.: Академия, 2009. – 272 с.
3. Запечников, С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности. – М.: Горячая линия-Телеком, 2007 – 320 с.
4. Єнікєєв, Р.І. Дослідження сучасних систем цифрового підпису / Р.І. Єнікєєв, В.О. Болтьонков. // Збірник матеріалів міжнародної наукової конференції «Сучасні інформаційні технології». – 2014 – С.21-22.
5. Nemati, H.R. Applied Cryptography for Cyber Security and Defence: Information Encryption and Cyphering / H.R. Nemati, L. Yang – N.-Y.: IGI Global, 2011– 383 p.
6. ДСТУ4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. – К.: Держстандарт України, 2003. –39 с.
7. Open SSL: [Электронный ресурс] // Режим доступ: https://www.openssl.org/ (Дата обращения: 01.08/2014).

ПРАКТИЧНЕ ДОСЛІДЖЕННЯ СУЧАСНИХ СИСТЕМ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

В.О. Болтьонков, Р.І.Єнікєєв

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

Досліджено сучасні алгоритми електронного цифрового підпису (ЕЦП). Алгоритми проаналізовані з точки зору зручності програмної реалізації та швидкодії на різних етапах ЕЦП. Досліджено найбільш застосовувані криптографічні хеш-функції як складова частина системи ЕЦП. Дослідження проведене шляхом програмної реалізації різних систем ЕЦП на мові Java с використанням бібліотеки Open SSL та подальшим програмним профілюванням.

Ключові слова: електронний цифровий підпис, хеш-функція, стандарти цифрового підпису, асиметричні криптографічні системи, швидкодія.

RESEARCH OF MODERN DIGITAL SIGNATURE SYSTEMS

V.O. Boltenkov, R.I. Yenikyeyev

Odessa National Polytechnical University,
1, Shevchenko ave., Odessa, 65044, Ukraine; e-mail: vaboltenkov@mail.ru

Modern digital signature (DS) systems were researched. The DS algorithms were analyzed with respect to easiness of software implementation and speed related to their different stages. Common cryptographic hash functions were researched as a part of a DS system. The research was performed by means of Java software implementation of different DS systems with the use of OpenSSL toolkit and further software profiling.

Keywords: digital signature, hash function, digital signature standards, asymmetric cryptographic systems, algorithm speed.

УДК 621.391:004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 3, pp. 210-218

МЕТОД КРИПТОГРАФИЧЕСКОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ НА БАЗЕ ЭКВИВАЛЕНТНОГО КЛАССА СОВЕРШЕННЫХ ДВОИЧНЫХ РЕШЕТОК

Н.И. Кушниренко, В.Я. Чечельницкий

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

На основе свойств совершенных двоичных решеток эквивалентного класса предложен криптографический метод передачи информации, который позволяет уменьшить сложность декодера за счет применения единственного, перестраиваемого под порождающую решетку согласованного фильтра, обеспечить параметрическую скрытность передачи информации, помехоустойчивое кодирование и организовать многоканальную систему передачи информации.

Ключевые слова: криптографическая передача информации, совершенные двоичные решетки, метод модуляции, широкополосные сигналы

Введение

На радиоканал передачи данных, как на открытую систему, в общем случае воздействуют помехи и многолучевые замирания, вызванные естественным происхождением, а также канал подвержен воздействию помех искусственного происхождения от систем преднамеренного разрушения информации, подавления или перехвата данных.

Таким образом, современные системы передачи информации должны противостоять воздействию как естественных, так и специально организованных помех, т.е. обладать высокой помехозащищенностью.

Помехозащищенность – это главный комплексный показатель качества работы систем передачи информации, который включает [1]: помехоустойчивость, энергетическую скрытность, структурную или параметрическую скрытность, криптостойкость, имитостойкость, защиту информации от преднамеренных помех, подавления и перехвата сигналов, защиту информации от несанкционированного доступа. Поэтому главной проблемой телекоммуникационных систем является повышение помехозащищенности.

Обычно проблемы защиты передаваемой информации от влияния помех в каналах связи и защиты информации от несанкционированного доступа решаются независимо. Для защиты информации от воздействия природных и искусственно создаваемых помех используются методы помехоустойчивого кодирования, основанные на внесении передающим устройством в передаваемые цифровые сигналы избыточности и использовании этой избыточности приемником для исправления возникших в канале связи ошибок. А для защиты информации от несанкционированного доступа используются различные методы шифрования.

Для защиты передаваемой информации от влияния помех в каналах связи можно применить совершенные двоичные решетки – СДР. На базе СДР можно строить классы двумерных корректирующих кодов [2]. СДР можно применять и для криптографической передачи информации [3].

Цель статьи и постановка исследований

Целью настоящей статьи является разработка метода криптографической передачи информации с помощью объединения шифрования и канального кодирования на базе эквивалентного класса совершенных двоичных решеток.

Для достижения цели необходимо решить следующие *задачи*:

1. Рассмотреть свойства СДР эквивалентного класса при выполнении операций циклического сдвига строк и столбцов.
2. Разработать принцип и схему информационной модуляции и демодуляции на основе циклических сдвигов СДР эквивалентного класса.
3. Разработать схему модема для криптографической передачи информации.
4. Рассмотреть требования к блокам модема криптографической передачи информации.

Исследования, приведенные в данной статье, выполнены в рамках НИР «Методы защиты информации в широкополосных телекоммуникационных системах» проводимых кафедрой информационной безопасности Одесского национального политехнического университета.

Основная часть

Каждая СДР порядка N порождает класс эквивалентных матриц – $E(N)$-класс СДР [4], путем использования операций циклического сдвига строк и/или столбцов, при этом мощность $E(N)$-класса эквивалентных матриц определяется выражением

$$\Psi_{E(N)} = N^2. \tag{1}$$

Таким образом, если каким-либо способом построена СДР, то тем самым, по сути, задан класс эквивалентных СДР мощности (1), который можно построить из этой СДР как из порождающей.

В табл. 1, в качестве примера, представлен эквивалентный $E(4)$-класс СДР, который построен на базе порождающей матрицы

$$P(4) = \begin{bmatrix} + & + & - & - \\ + & + & + & + \\ - & + & + & - \\ - & + & - & + \end{bmatrix}. \tag{2}$$

Здесь символом «+» обозначен элемент СДР «+1», символом «–» обозначен элемент СДР «–1» для краткости. Далее мы будем применять те же обозначения.

Индексы $[k1, k2]$ возле имени СДР (табл. 1) указывают, на какое количество позиций циклически сдвинуты строки и/или столбцы порождающей СДР – $P^{[0,0]}(4)$, причем $k1$ обозначает количество позиций сдвига строк вниз, а $k2$ — количество позиций сдвига столбцов вправо.

Введем понятие двумерной периодической взаимнокорреляционной функции (ДПВКФ) между произвольными СДР $P^0(N)$ и $P^1(N)$

$$B(N) = \left\| b_{m,n} \right\|, \tag{3}$$

при этом элементы ДПВКФ (3) между двумя СДР $P^0(N)$ и $P^1(N)$ вычисляются по формуле

$$b_{m,n} = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} p^0_{i,j} p^1_{i+m,j+n}. \qquad (4)$$

Таблица 1.

Эквивалентный $E(4)$-класс СДР

	$k2=0$	$k2=1$	$k2=2$	$k2=3$
$k1=0$	$P^{[0,0]}(4)=\begin{bmatrix}+&+&-&-\\+&+&+&+\\-&+&+&-\\-&+&-&+\end{bmatrix}$	$P^{[0,1]}(4)=\begin{bmatrix}-&+&+&-\\+&+&+&+\\-&-&+&+\\+&-&+&+\end{bmatrix}$	$P^{[0,2]}(4)=\begin{bmatrix}-&-&+&+\\+&+&+&+\\+&-&-&+\\-&+&-&+\end{bmatrix}$	$P^{[0,3]}(4)=\begin{bmatrix}+&-&-&+\\+&+&+&+\\+&+&-&-\\+&-&+&-\end{bmatrix}$
$k1=1$	$P^{[1,0]}(4)=\begin{bmatrix}-&+&-&+\\+&+&-&-\\+&+&+&+\\-&+&+&-\end{bmatrix}$	$P^{[1,1]}(4)=\begin{bmatrix}+&-&+&-\\-&+&+&-\\+&+&+&+\\-&-&+&+\end{bmatrix}$	$P^{[1,2]}(4)=\begin{bmatrix}-&+&-&+\\-&-&+&+\\+&+&+&+\\+&-&-&+\end{bmatrix}$	$P^{[1,3]}(4)=\begin{bmatrix}+&-&+&-\\+&-&-&+\\+&+&+&+\\+&+&-&-\end{bmatrix}$
$k1=2$	$P^{[2,0]}(4)=\begin{bmatrix}-&+&+&-\\-&+&-&+\\+&+&-&-\\+&+&+&+\end{bmatrix}$	$P^{[2,1]}(4)=\begin{bmatrix}-&-&+&+\\+&-&+&-\\-&+&+&-\\+&+&+&+\end{bmatrix}$	$P^{[2,2]}(4)=\begin{bmatrix}+&-&-&+\\-&+&-&+\\-&-&+&+\\+&+&+&+\end{bmatrix}$	$P^{[2,3]}(4)=\begin{bmatrix}+&+&-&-\\+&-&+&-\\+&-&-&+\\+&+&+&+\end{bmatrix}$
$k1=3$	$P^{[3,0]}(4)=\begin{bmatrix}+&+&+&+\\-&+&+&-\\-&+&-&+\\+&+&-&-\end{bmatrix}$	$P^{[3,1]}(4)=\begin{bmatrix}+&+&+&+\\-&-&+&+\\+&-&+&-\\-&+&+&-\end{bmatrix}$	$P^{[3,2]}(4)=\begin{bmatrix}+&+&+&+\\+&-&-&+\\-&+&-&+\\-&-&+&+\end{bmatrix}$	$P^{[3,3]}(4)=\begin{bmatrix}+&+&+&+\\+&+&-&-\\+&-&+&-\\+&-&-&+\end{bmatrix}$

В табл. 2, в качестве примера, приведены ДПВКФ между порождающей СДР (2) порядка $N=4$ с параметрами циклического сдвига строк и столбцов – $[0,0]$ и всеми остальными матрицами эквивалентного $E(4)$-класса СДР из табл. 1 с параметрами сдвига $[k1,k2]$.

Из рассмотрения табл. 1 и табл. 2 следует важное свойство СДР эквивалентного $E(N)$-класса.

Свойство. ДПВКФ между порождающей СДР и СДР, чьи строки и/или столбцы циклически сдвинуты по отношению к ней, содержит один пик, энергия которого равна $E=N^2$. Сдвиги этого пика, по отношению к местоположению его в ДПАКВ, однозначно определяют количество циклических сдвигов строк и/или столбцов СДР относительно порождающей СДР.

Таблица 2.

ДПВКФ между СДР эквивалентного $E(4)$ -класса

$B^{[0,0]}(4) = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[0,1]}(4) = \begin{bmatrix} 0 & 16 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[0,2]}(4) = \begin{bmatrix} 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[0,3]}(4) = \begin{bmatrix} 0 & 0 & 0 & 16 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$
$B^{[1,0]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[1,1]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 16 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[1,2]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[1,3]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 16 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$
$B^{[2,0]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[2,1]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 16 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[2,2]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$B^{[2,3]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 16 \\ 0 & 0 & 0 & 0 \end{bmatrix}$
$B^{[3,0]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 \end{bmatrix}$	$B^{[3,1]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 16 & 0 & 0 \end{bmatrix}$	$B^{[3,2]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 16 & 0 \end{bmatrix}$	$B^{[3,3]}(4) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 16 \end{bmatrix}$

Установленное свойство имеет важное практическое значение, поскольку является, по сути, обоснованием метода передачи информации на основе циклических сдвигов порождающей СДР.

Рассмотрим более подробно метод передачи информации, основанный на циклических сдвигах СДР эквивалентного $E(N)$ -класса. Схема модулятора, функционирующая на его основе, показана на рис. 1.

Предположим, что сообщение состоит из дискретных символов, каждый из которых выбран из некоторого конечного множества – алфавита. Пусть

$$A \in \{a_0, a_1, a_2, \ldots, a_i, \ldots, a_{q-1}\} \tag{5}$$

алфавит, состоящий из q разных символов. Для передачи каждого символа a_i, где i – номер соответствующего символа из алфавита A (5), модулятор будет использовать одну порождающую СДР из $E(N)$ -класса.

Счетно-решающее средство определения количества циклических сдвигов строк и столбцов работает в модульной арифметике и, соответственно, рассчитывает параметры $k1$ и $k2$ по номеру i передаваемого символа a_i, для передаваемой СДР, следующим образом

$$k1 = Int(i / N), \tag{6}$$

где $Int(a/b)$ – означает целую часть от деления a на b;

$$k2 = Res(i/N), \tag{7}$$

где $Res(a/b)$ – означает остаток от деления a на b.

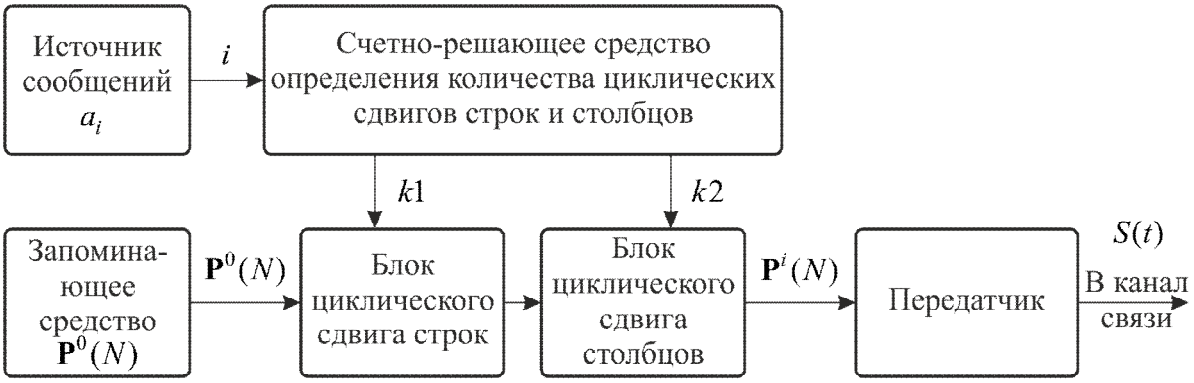


Рис. 1. Модулятор сигналов на основе СДР

Ясно, что порядок N для СДР $E(N)$-класса необходимо выбирать из условия $N^2 \geq q$.

Блок циклического сдвига строк производит циклический сдвиг порождающей СДР $P^0(N)$ на $k1$ (9) строк вниз. Блок циклического сдвига столбцов производит циклический сдвиг полученной СДР на $k2$ (10) столбцов вправо.

При этом каждому передаваемому символу a_i из некоторого алфавита мощности N^2 ставится в соответствие одна СДР из используемого эквивалентного $E(N)$-класса. Номер i соответствующего символа a_i определяет количество циклических сдвигов строк и/или столбцов порождающей СДР $P^0(N)$.

В результате такой информационной модуляции получаем двумерное кодовое слово, которое последовательно строка за строкой подается на вход передатчика, где осуществляется (вторая ступень модуляции) частотная или фазовая модуляция (манипуляция) несущей частоты. Таким образом, в канал связи излучается одномерный дискретный сигнал $S(t)$, длины $n = N^2$ элементов. Ясно, что база такого сигнала определяется как

$$B = FT = N^2, \tag{8}$$

где N – порядок СДР.

Сложность радиотехнических устройств обычно оценивают количеством элементов памяти и количеством сумматоров, так как именно эти элементы влияют на быстродействие устройства и его цену. Заметим, что в передающем устройстве хранится одна порождающая СДР, вместо N^2 СДР эквивалентного класса, как это обычно происходит при традиционных методах передачи информации, поэтому ориентировочно сложность предложенного модулятора в N^2 меньше по количеству элементов в сравнении с модемами, которые построены по традиционным схемам.

В приемной части системы телекоммуникаций (рис. 2) осуществляется обработка принятого в условиях помех $\xi(t)$ сигнала $y(t)$

$$y(t) = S(t) + \xi(t).$$

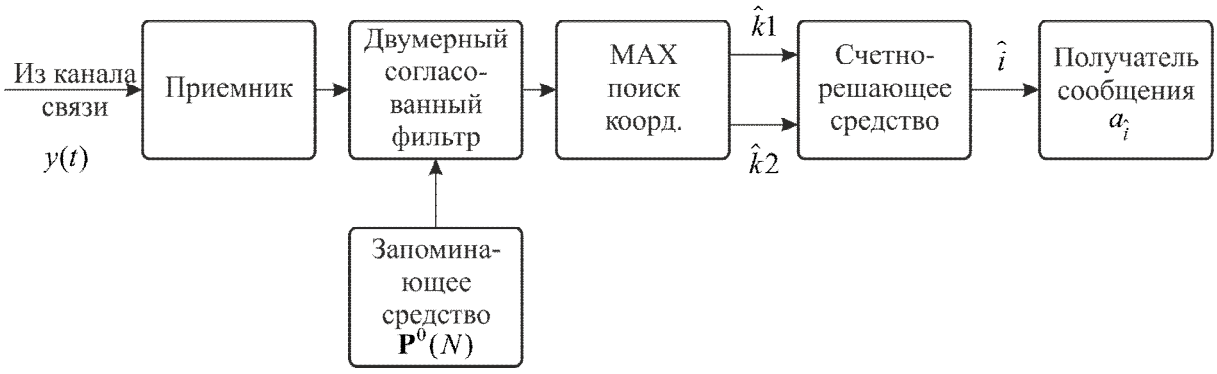


Рис. 2. Демодулятор сигналов на основе СДР

Вначале в приемнике осуществляется поэлементный прием сигнала $y(t)$ и формирование принятой решетки $Y(N)$. В демодуляторе (декодере) с корреляционным методом декодирования с помощью двумерного согласованного фильтра проводится расчет ДПВКФ между принятой решеткой $Y(N)$ и порождающей решеткой $P^0(N)$, параметры последней хранятся в запоминающем средстве. Затем решающее средство декодера осуществляет поиск максимального лепестка ДПВКФ и значений его максимально правдоподобных координат $(\hat{k}1, \hat{k}2)$.

Декодер источника вычисляет номер максимально правдоподобного передаваемого символа следующим образом

$$\hat{i} = \hat{k}1 \cdot N + \hat{k}2. \qquad (9)$$

Максимально правдоподобный номер $\hat{i}$ определяет переданное сообщение $a_{\hat{i}}$, которое поступает получателю сообщения.

Следует заметить, что декодирование сигналов, построенных на базе эквивалентного $E(N)$-класса СДР мощности N^2, можно осуществить с помощью единственного двумерного согласованного с порождающей СДР фильтра, вместо N^2 фильтров, как это требуется в общем случае при построении многоканального приемника и схемы поиска координат главного пика ДПВКФ.

Общая блок-схема модема на основе СДР показана на рис. 3.

На первый взгляд может показаться, что предложенный модем на базе СДР обеспечивает криптографический метод передачи информации. Ведь ни один бит передаваемого номера символа не связан никакими математическими преобразованиями с передаваемым по каналу связи кодом. Понятно, что если криптоаналитику не известно, какая СДР эквивалентного $E(N)$-класса была установлена в качестве базовой, то в этом случае невозможно определить какие были параметры циклического сдвига строк $(k1)$ и столбцов $(k2)$ и, соответственно, невозможно определить какой номер символа был передан.

Однако вскрытие представленного способа передачи информации, для криптоаналитика, не составляет больших трудностей, так как данный метод передачи информации представляет собой обычный шифр подстановки, т.е. код передаваемого символа заменяется на соответствующую СДР.

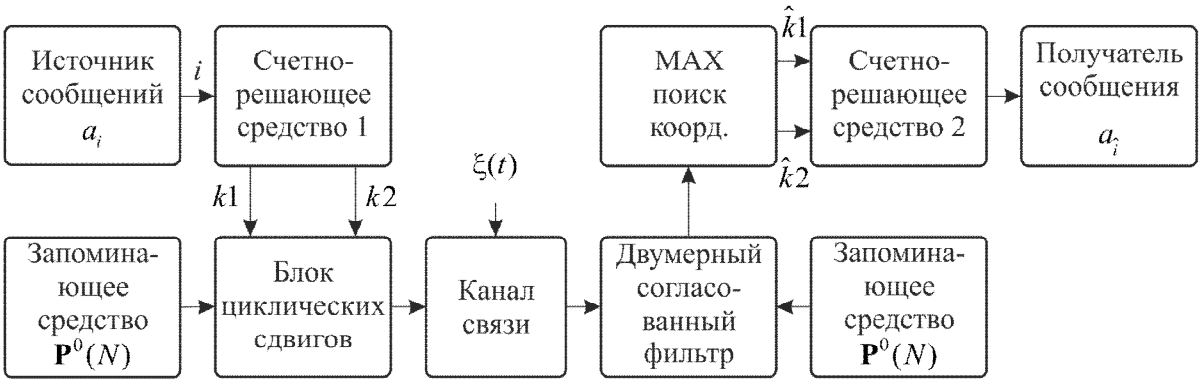


Рис. 3. Блок-схема модема на основе СДР

После приема некоторого кодированного сообщения, нетрудно определить относительную частоту появления различных СДР и поставить эту частоту в соответствие со среднестатистическими данными появления букв алфавита в тексте соответствующего языка.

Зная алгоритм передачи информации, алфавит, формулы для вычисления параметра сдвига строк и столбцов (6), (7), (9), по одному правильно определенному символу легко определить базовую СДР и после этого получить весь открытый текст.

Для того чтобы метод передачи информации не поддавался дешифрованию, необходимо, чтобы для каждого нового передаваемого символа открытого текста использовалась новая порождающая СДР. Это можно осуществить путем добавления в предложенную схему передатчика (рис. 1) и приемника (рис. 2) генератора эквивалентного класса СДР вместо запоминающего средства $P^0(N)$ (рис. 4).

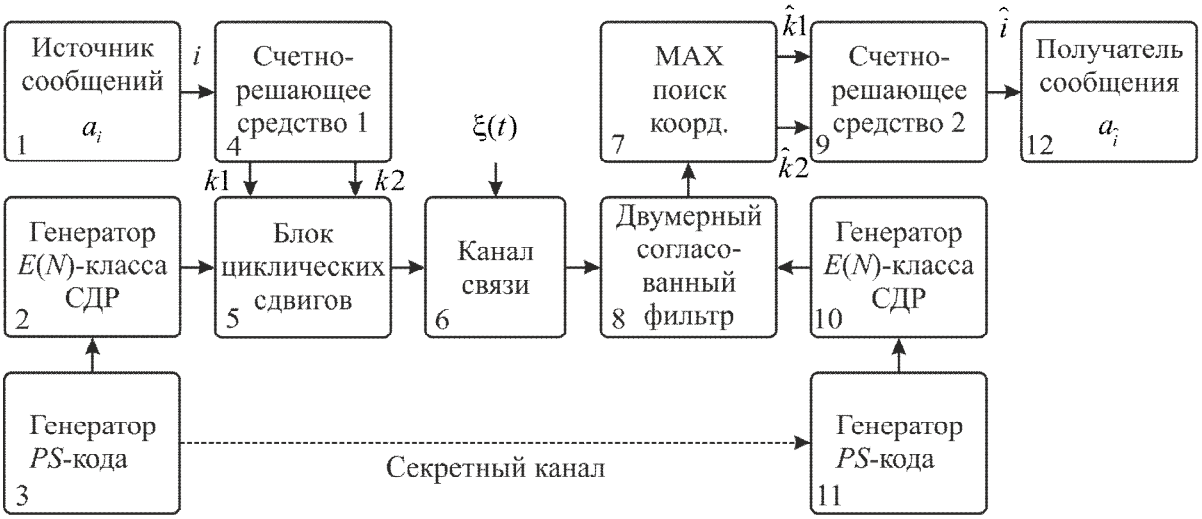


Рис. 4. Блок-схема модема на основе $E(N)$ -класса СДР

Генератор $E(N)$ -класса СДР (блок 2, блок 10), который управляется генератором PS -кода (блок 3, блок 11), для каждого очередного символа открытого сообщения (блок 1) генерирует новую порождающую СДР. Генератор PS -кода (блок 3, блок 11) формирует псевдослучайные числа, последовательность которых управляется закрытым ключом, передающимся на приемную сторону по секретному каналу.

Закрытый ключ изменяет параметры генератора PS-кода. Остальная часть схемы работает так же, как было описано ранее.

Рассмотрим требования к генератору $E(N)$-класса СДР (блок 2 и блок 10). Данный генератор должен генерировать все СДР заданного эквивалентного класса, который определяется порождающей СДР. Структура генерируемой СДР определяется ее номером, который является целочисленным значением и подается на генератор от внешнего устройства в двоичном виде. СДР нумеруются от 0 до $\Psi_{E(N)}-1$ (1), поэтому количество разрядов двоичного номера генерируемой СДР определяется выражением

$$l_{E(N)} = \log_2 \Psi_{E(N)}. \qquad (10)$$

Генератор PS-кода (блок 3, блок 11) должен формировать псевдослучайную последовательность, каждое значение которой должно иметь количество разрядов, которое определено в (10). Генератор PS-кода должен вырабатывать неповторяющуюся последовательность большой длины. После того, как будет осуществлена передача символов открытого текста (блок 1), количество которых равно длине последовательности, необходимо сформировать новый закрытый ключ, который изменит параметры генераторов PS-кода (блоки 3 и 11).

В связи с тем, что для передачи очередного символа открытого текста каждый раз используется новая порождающая СДР, в канале связи (блок 6) появляются статистически независимые СДР. Криптоаналитик может получить информацию только о том, что по каналу связи передан какой-то символ из заданного алфавита (5). Другая информация ему не доступна.

При достаточной базе (8) шумоподобного сигнала, который сформирован на основе СДР и передается по каналу связи (блок 6), мощность сигнала может быть ниже мощности естественных шумов канала связи. Простым энергетическим приемником в таких условиях невозможно определить даже факт передачи информации. Для перехвата таких сигналов необходимо знать структуру этих сигналов, а она для каждого передаваемого символа открытого текста постоянно изменяется. Кроме того, необходимо обратить внимание на то, что шумоподобные сигналы, которые построены на базе СДР, обладают большой избыточностью.

Каждая СДР может содержать максимум N^2 бит информации, однако фактически переносит только $\log_2 N^2$. Таким образом, относительная скорость r передачи информации рассмотренной схемы составляет

$$r = \frac{\log_2 N^2}{N^2}.$$

Такая избыточность кода позволяет исправлять ошибки, которые могут возникнуть в канале связи при передаче информации.

Рассмотренный метод криптографической передачи информации позволит создать и многоканальную систему передачи информации, если в качестве порождающих использовать минимаксные совершенные двоичные решетки.

Выводы

В работе рассмотрены свойства СДР при выполнении операций циклического сдвига строк и/или столбцов и свойства двумерных периодических взаимнокорреляционных функций между СДР эквивалентного $E(N)$-класса.

На основе рассмотренных свойств СДР обоснован выбор метода информационной модуляции на базе эквивалентного класса СДР. Приведены структурные схемы модулятора и демодулятора сигналов на основе СДР. Показано, что сложность построения модулятора и демодулятора (модема) уменьшена приблизительно в N^2 по сравнению с традиционными схемами.

Предложена модификация указанного модема для осуществления криптографической передачи информации.

Результаты, полученные в данной работе, могут быть использованы при построении многоканального криптографического модема, который может обеспечить параметрическую скрытность передачи информации и исправление ошибок, которые могут возникнуть в канале связи.

Список литературы

1. Варакин, Л.Е. Системы связи с шумоподобными сигналами / Л.Е. Варакин. — М.: Радио и связь, 1985. — 384 с.
2. Баранов, П.Е. Класс двумерных корректирующих кодов на основе совершенных двоичных решеток / П.Е. Баранов, М.И. Мазурков, В.Я. Чечельницкий, А.А. Яковенко // Радиоэлектроника (Изв. вузов).— 2009.— Т. 52, № 2.— С. 29–35.
3. Мазурков, М.И. Метод защиты информации на основе совершенных двоичных решеток / М.И. Мазурков, В.Я. Чечельницкий, П. Мурр // Радиоэлектроника (Изв. вузов).— 2008.— Т. 51, № 11.— С. 53–57.
4. Мазурков, М.И. Классы эквивалентных и порождающих совершенных двоичных решеток для CDMA-технологий / М.И. Мазурков, В.Я. Чечельницкий // Радиоэлектроника (Изв. вузов).— 2003.— Т. 46, № 5.— С. 54–63.

МЕТОД КРИПТОГРАФІЧНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ НА БАЗІ ЕКВІВАЛЕНТНОГО КЛАСУ ДОСКОНАЛИХ ДВІЙКОВИХ РЕШІТОК

Н.І. Кушніренко, В.Я. Чечельницький

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

На основі властивостей досконалих двійкових решіток еквівалентного класу запропоновано криптографічний метод передачі інформації, який дозволяє зменшити складність декодера за рахунок застосування єдиного узгодженого фільтра, який перебудовується під породжуючу решітку, забезпечити параметричну скритність передачі інформації, завадостійке кодування і організувати багатоканальну систему передачі інформації.

Ключові слова: криптографічна передача інформації, досконалі двійкові решітки, метод модуляції, широкосмугові сигнали

METHOD OF CRYPTOGRAPHIC DATA TRANSFER BASED ON EQUIVALENT CLASS OF PERFECT BINARY LATTICES

N.I. Kushnirenko, V. Ia. Chechelnytskyi

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: natalka_kni@ukr.net

A cryptographic data transfer method was developed based on the features of perfect binary lattices of equivalent class. This method allows for the following: (1) simplification of the decoder structure due to the use of single matched filter redeveloped for generic lattice, (2) parametric data transfer security, (3) robust coding, and (4) organization of multichannel data transfer.

Keywords: cryptographic data transfer, perfect binary lattices, modulation method, broadband signals.

UDC 681.513

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 3, pp. 219-224

A TECHNIQUE TO SOLVE THE PROBLEM OF PARAMETRIC IDENTIFICATION OF MATHEMATICAL MODELS OF ANOMALOUS FLUIDS FILTRATION PROCESSES IN POROUS MEDIA

S.A. Polozhaenko, A.A. Fomin

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: polozhaenko@mail.ru

The problem of parametric identification of mathematical models (MM) of reservoir systems for the porosity and permeability functions of ground rock (medium) was defined. A technique to solve the problem of parametric identification of the MM class under study was proposed based on the gradient projection method with minimization of the squared quality criterion.

Keywords: anomalous liquids, mathematical model, parametric identification, functional, quality criterion, gradient projection method.

Introduction

In some important industries such as construction industry, mining and geological prospecting, modeling of filtration fluid flows is required. Here the complexity of mathematical models (MM) of filtration flows is determined, among other factors, by a number of fluids subjected to filtration (i.e., number or phases), their fractional make-ups, and geological soil structure. The MM proposed in [1,2] as a variational inequality with proper boundary and initial conditions may be considered as an adequate MM for mutual filtration of a viscous (ideal) fluid and viscoplastic (anomalous) fluid. It should be noted that the porosity $m(\bar{z})$ and permeability functions $k_i(\bar{z}), i = 1,2$ of the medium (reservoir rock) are used as the parameters of this MM. Hereinafter, indices $i = 1,2$ define fluids subjected to filtration. On frequent occasions, the values of these parameters are not known, and the problem of their determination is a complex autonomous problem of investigation of a reservoir system, the problem of parametric identification.

The *purpose* of this work was to develop a constructive computational procedure for identification of the porosity and permeability functions of the formation.

Statement of a problem

According to [1], an incremental MM for mutual filtration of a viscous (ideal) liquid and viscoplastic (anomalous) fluid may be represented as

$$-\frac{m\partial(\Delta S_2)}{\partial t}-\int_\Omega\sum_{i=1}^{n}\left[k_1\frac{\partial^2(\Delta P)}{\partial z_i^2}|\Delta v|\right]dz+\int_\Omega\sum_{i=1}^{n}\left[k_1\frac{\partial^2(\Delta P)}{\partial z_i^2}|\Delta S_2|\right]dz\geq\frac{1}{h}\sum_{j=1}^{K_1}\zeta_j(z)Q_{1_j},\quad \forall v,\ S_2\in K, \tag{1}$$

$$-\frac{m\partial(\Delta S_2)}{\partial t}-\int_\Omega\sum_{i=1}^{n}\left(k_2\frac{\partial^2(\Delta P)}{\partial z_i^2}\right)dz=\frac{1}{h}\sum_{j=1}^{K_2}\zeta_j(z)Q_{2_j}, \tag{2}$$

$$\Delta P(0,z)=\Delta P_0(z),\ \Delta S_2(0,z)=\Delta S_{2_0}(z), \tag{3}$$

$$\frac{\partial[\Delta S_2(t,z)]}{\partial\eta}\geq 0;\ S_2(t,z)<S_{2_{\max}}, \tag{4}$$

$$\frac{\partial[\Delta S_2(t,z)]}{\partial\eta}=0;\ S_2(t,z)\geq S_{2_{\max}}, \tag{5}$$

where $P=P(t,z)$ is the intrastratal pressure, $S_2=S_2(t,z)$ is the reservoir saturation with displacing fluid, $v=v(t,z)$ is the test function, h is bulk of reservoir rock, K is the set at which $S_2=S_2(t,z)$ and $v=v(t,z)$ functions are defined, K_1,K_2 are a number of production and injection wells, respectively; Q_1,Q_2 are the debits of corresponding wells, $\zeta(z)$ is the Dirac function, η is the normal to the boundary. Let us assign the following functional as a quality criterion for the solution of identification problem:

$$J_1[m(\cdot),k_1(\cdot)]=\sum_{j=1}^{K_1+K_2}\left\{\int_{T_j}\left[P'(t,z_j,m,k_1)-F_j^P(t)\right]^2dt+\int_{T_j}\left[S_2{}'(t,z_j,m,k_1)-F_j^S(t)\right]^2dt\right\}, \tag{6}$$

where $P'(\cdot)$ and $S_2{}'(\cdot)$ are the exact values of the functions of intrastratal pressure and the reservoir saturation with displacing fluid, respectively, F^P and F^S are the measured values of the specified functions, and T is the period of time when the measurement is done.

Proof of the differentiability of the quality criterion

Let us show that the quality criterion assigned will be differentiable in any point of the spatial domain $\bar{z}\in\Omega$ (including its boundary G), i.e, that the increment (6) equal to

$$\Delta J_1=J_1[(m+h^m),(k_1+h^k)]-J_1(m,k_1)$$

is presentable as

$$\Delta J_1=\int_\Omega\{[J'(m,k_1)h^m]dz+[J'(m,k_1)h^k]dz\}+\left[O\left(\left\|h^m\right\|_{L^2}\right)+O\left(\left\|h^k\right\|_{L^2}\right)\right], \tag{7}$$

where $J'(m,k_1)$ is a function from $L^2(\Omega)$, $O\left(\left\|h^m\right\|_{L^2}\right)$ and $O\left(\left\|h^k\right\|_{L^2}\right)$ are the remainders such that $\lim\limits_{\alpha^m\to+0}O(\alpha^m)(\alpha^m)^{-1}=0$, $\lim\limits_{\alpha^k\to+0}O(\alpha^k)(\alpha^k)^{-1}=0$.

Let us re-write the functional increment ΔJ_1 in a formal way as follows:

$$\Delta J_1 = \sum_{j=1}^{K_1+K_2} \left\{ \int_\Omega \left\{ \left[P(t,z_j,m,k_1) + \Delta P(t,z_j) - F_j^P(t) \right]^2 - \right.\right.$$

$$- \left[P(t,z_j,m,k_1) - F_j^P(t) \right]^2 \Big\} dz + \Big\{ \left[S_2(t,z_j,m,k_1) + \Delta S_2(t,z_j) - F_j^S(t) \right]^2 -$$

$$\left.\left. + \left\{ \left[S_2(t,z_j,m,k_1) + \Delta S_2(t,z_j) - F_j^S(t) \right]^2 - \left[S_2(t,z_j,m,k_1) - F_j^S(t) \right]^2 \right\} dz \right\} =$$

$$= \sum_{j=1}^{K_1+K_2} \left\{ \int_\Omega \left\{ \left\{ \left[P(t,z_j,m,k_1) - F_j^P(t) \right] + \Delta P(t,z_j) \right\}^2 - \right.\right.$$

$$- \left[P(t,z_j,m,k_1) - F_j^P(t) \right] \Big\} dz + \Big\{ \left\{ \left[S_2(t,z_j,m,k_1) - F_j^S(t) \right] + \Delta S_2(t,z_j) \right\}^2 - \quad (8)$$

$$\left.\left. - \left[S(t,z_j,m,k_1) - F_j^S(t) \right] \right\} dz \right\} =$$

$$= \sum_{j=1}^{K_1+K_2} \left\{ \left\{ \int_\Omega 2 \left[P(t,z_j,m,k_1) - F_j^P(t) \right] \Delta P(t,z) dz + \int_\Omega \Delta P^2(t,z_j) dz \right\} + \right.$$

$$\left. + \left\{ \int_\Omega 2 \left[S_2(t,z_j,m,k_1) - F_j^S(t) \right] \Delta S_2(t,z) dz + \int_\Omega \Delta S_2^2(t,z_j) dz \right\} \right\}.$$

Now let us convert this expression to the form of (7). To this end, let us introduce functions $p_P^*(t,z) \equiv p_P^*(t,z,m,k_1)$ and $p_S^*(t,z) \equiv p_S^*(t,z,m,k_1)$ into consideration as solutions of the following boundary-value problem

$$- \frac{m \partial p_S^*}{\partial t} (v - S_2) - \int_\Omega \sum_{i=1}^n \left[k_1 \frac{\partial^2 p_P^*}{\partial z_i^2} |v| \right] dz + \int_\Omega \sum_{i=1}^n \left[k_1 \frac{\partial^2 p_P^*}{\partial z_i^2} |S_2| \right] dz \geq \geq \frac{1}{h} \sum_{j=1}^{K_1} \zeta_j(z) Q_{1_j}, \quad (9)$$

$$\forall v, S_2 \in K,$$

$$- \frac{m \partial p_S^*}{\partial t} - \int_\Omega \sum_{i=1}^n \left(k_2 \frac{\partial^2 p_P^*}{\partial z_i^2} \right) dz = \frac{1}{h} \sum_{j=1}^{K_2} \zeta_j(z) Q_{2_j}, \quad (10)$$

$$\left. \frac{\partial p_S^*}{\partial \eta} \right|_{z=0} \geq 0; 0 \leq t \leq t_k, \quad (11)$$

$$p_P^* \big|_{t=t_k} = 2 \left[P(t_k,z_j,m,k_1) - F^P(t) \right], p_S^* \big|_{t=t_k} = 2 \left[S_2(t_k,z_j,m,k_1) - F^S(t) \right], \ \forall z \in \Omega. \quad (12)$$

While taking (1) – (5), (9) – (12) into account, the first integral in the first component of right-hand side of equation (8) is converted as follows

$$I_P = \int_\Omega 2 \left[P(t,z_j,m,k_1) - F_j^P(t) \right] \Delta P(t,z_j) dz = \int_\Omega p_P^*(t_k,z_j) \Delta P(t,z_j) dz =$$

$$= \int_{\Omega}\left[\int_0^{t_k}\frac{\partial}{\partial t}\left(p_P^*\Delta P\right)dt\right]dz = \int_{\Omega}\int_0^{t_k}\left[\frac{\partial p_P^*}{\partial t}\Delta P + p_P^*\frac{\partial(\Delta P)}{\partial t}\right]dtdz =$$

$$= \int_{\Omega}\int_0^{t_k}\left\{\frac{1}{m(z)}\left\{\sum_{i=1}^{n}\left[k_1(z_i)\frac{\partial^2 p_P^*}{\partial z_j^2}|v|\right] + \sum_{i=1}^{n}\left[k_1(z_i)\frac{\partial^2 p_P^*}{\partial z_j^2}|S_2|\right]\right\}\Delta P + \right.$$

$$\left. + p_P^*\left\{\sum_{i=1}^{n}\left[k_1(z_i)\frac{\partial^2 p_P^*}{\partial z_j^2}|\Delta v|\right] + \sum_{i=1}^{n}\left[k_1(z_i)\frac{\partial^2 p_P^*}{\partial z_j^2}|\Delta S_2|\right]\right\}\right\}dtdz\ .$$

Neglecting the last expression in spatial domain, we will obtain the following

$$I_P{}' = \int_0^{t_k}\left\{\frac{1}{m(z)}\left\{\sum_{i=1}^{n}\left[k_1(z_i)\frac{\partial^2 p_P^*}{\partial z_j^2}|v|\right] + \sum_{i=1}^{n}\left[k_1(z_i)\frac{\partial^2 p_P^*}{\partial z_j^2}|S_2|\right]\right\}\Delta P + \right.$$

$$\left. + p_P^*\left\{\sum_{i=1}^{n}\left[k_1(z_i)\frac{\partial^2 p_P^*}{\partial z_j^2}|v|\right] + \sum_{i=1}^{n}\left[k_1(z_i)\frac{\partial^2 p_P^*}{\partial z_j^2}|S_2|\right]\right\}\right\}\Bigg|_{\Omega} dt = \qquad (13)$$

$$= \int_0^{t_k}\frac{1}{m(z)}\left[\left(\sum_{i=1}^{n}k_1(z_i)p_P^*|v|\right) + \left(\sum_{i=1}^{n}k_1(z_i)p_P^*|S_2|\right)\right]\Delta P dt\ .$$

Similarly, for the expression in (8) written with respect to function $S_2(t,z)$ (i.e., the first integral in the second component of right-hand side of equation (8)), one may write the following

$$I_S = \int_{\Omega} 2\left[S_2(t,z_j,m,k_1) - F_j^S(t)\right]\Delta S_2(t,z_j)dz = \int_{\Omega} p_P^*(t_k,z_j)\Delta S_2(t,z_j)dz$$

or, omitting obvious conversions, when using integration in the spatial domain, finally we obtain the following

$$I_S{}' = \int_0^{t_k}\frac{1}{m(z)}\left[\left(\sum_{i=1}^{n}k_1(z_i)p_P^*|v|\right) + \left(\sum_{i=1}^{n}k_1(z_i)p_P^*|S_2|\right)\right]\Delta S_2 dt\ . \qquad (14)$$

Second integrals in the components of right-hand side of equation (8) are determined mostly by the terms of $\left[O\left(\|h\|_{L^2}^P\right) + O\left(\|h\|_{L^2}^S\right)\right]$ form presented in (7) and written for spatial problem statement. In this case,

$$\Delta J_1 = \int_{\Omega}\frac{1}{m(z)}\left[\left(\sum_{i=1}^{n}k_1(z_i)p_P^*|v|\right) + \left(\sum_{i=1}^{n}k_1(z_i)p_P^*|S_2|\right)\right]hdz + O\left(\|h\|_{L^2}\right). \qquad (15)$$

Determining the functional increment and forming the calculated relationships

As a result, the increment of functional (6) is represented as the following expression

$$\Delta J_1 = \int_0^{t_k} \frac{1}{m(z)} \left[\left(\sum_{i=1}^{n} k_1(z_i) p_P^* |v| \right) + \left(\sum_{i=1}^{n} k_1(z_i) p_P^* |S_2| \right) \right] h dz + O\left(\|h\|_{L^2} \right).$$

Therefore, the desired presentation (7) for functional (6) has been obtained, and the gradient of this functional has the following form

$$J_1'[m(z), k_1(z)] \equiv \frac{1}{m(z)} \left\{ \sum_{i=1}^{n} \left[k_1(z_i) p_P^* |v| \right] + \sum_{i=1}^{n} \left[k_1(z_i) p_P^* |S_2| \right] \right\}, \quad \forall z \in \Omega, \forall t \in [0, t_k]. \tag{16}$$

Then, with the gradient (16) available and using the procedure of gradient projection method [3] determined by relationships $U = \left\{ u(t) : u(t) \in L^2[0, t_k],\ a \le u(t) \le b,\ \forall t \in [0, t_k] \right\}$,

$$\Pr_u[u(t)] = \begin{cases} u(t),\ a \le u(t) \le b, \\ a,\ u(t) < a, \\ b,\ u(t) > b, \end{cases}$$

we obtain the final calculated relationships for identifiable functions $m(z)$ and $k_1(z)$

$$m_{q+1}(z) = \begin{cases} m_q(z) - \dfrac{\alpha_m}{m(z)} \left\{ \sum\limits_{i=1}^{n} \left[k_1(z_i) p_P^* |v| \right] + \sum\limits_{i=1}^{n} \left[k_1(z_i) p_P^* |S_2| \right] \right\}, \\ m_{\min} \le m_q(z) - \dfrac{\alpha_m}{m(z)} \left\{ \sum\limits_{i=1}^{n} \left[k_1(z_i) p_P^* |v| \right] + \sum\limits_{i=1}^{n} \left[k_1(z_i) p_P^* |S_2| \right] \right\} \le m_{\max}, \\ m_{\min}, \\ m_q(z) - \dfrac{\alpha_m}{m(z)} \left\{ \sum\limits_{i=1}^{n} \left[k_1(z_i) p_P^* |v| \right] + \sum\limits_{i=1}^{n} \left[k_1(z_i) p_P^* |S_2| \right] \right\} < m_{\min}, \\ m_{\max}, \\ m_q(z) - \dfrac{\alpha_m}{m(z)} \left\{ \sum\limits_{i=1}^{n} \left[k_1(z_i) p_P^* |v| \right] + \sum\limits_{i=1}^{n} \left[k_1(z_i) p_P^* |S_2| \right] \right\} > m_{\max}. \end{cases}$$

$$k_{1_{q+1}}(z) = \begin{cases} k_{1_q}(z) - \dfrac{\alpha_k}{m(z)} \left\{ \sum\limits_{i=1}^{n} \left[k_1(z_i) p_P^* |v| \right] + \sum\limits_{i=1}^{n} \left[k_1(z_i) p_P^* |S_2| \right] \right\}, \\ k_{1_{\min}} \le k_{1_q}(z) - \dfrac{\alpha_k}{m(z)} \left\{ \sum\limits_{i=1}^{n} \left[k_1(z_i) p_P^* |v| \right] + \sum\limits_{i=1}^{n} \left[k_1(z_i) p_P^* |S_2| \right] \right\} \le k_{1_{\max}}, \\ m_{\min}, \\ k_{1_q}(z) - \dfrac{\alpha_k}{m(z)} \left\{ \sum\limits_{i=1}^{n} \left[k_1(z_i) p_P^* |v| \right] + \sum\limits_{i=1}^{n} \left[k_1(z_i) p_P^* |S_2| \right] \right\} < k_{1_{\min}}, \\ m_{\max}, \\ k_{1_q}(z) - \dfrac{\alpha_k}{m(z)} \left\{ \sum\limits_{i=1}^{n} \left[k_1(z_i) p_P^* |v| \right] + \sum\limits_{i=1}^{n} \left[k_1(z_i) p_P^* |S_2| \right] \right\} > k_{1_{\max}} \end{cases}$$

Conclusions

The numerical investigations performed showed that the procedure proposed for sequential search of the porosity $m(\bar{z})$ and permeability $k_i(\bar{z}), i = 1,2$ has a high convergence rate (thus, e.g., to identify the parameters of a reservoir defined by the spatial sampling grid $z_1 = 12, z_2 = 16$, a sequence of no more than 8 iterations is required), with the total problem solving time of no more than 120 s.

References

1. Положаенко, С. А. Математические модели процессов течения аномальных жидкостей / С.А. Положаенко. // Моделювання та інформаційні технології: Зб. наук. праць. — К.: ІПМЕ, 2001. — Вип. 9. — С. 14 — 21.
2. Положаенко, С. А. Математическая модель фильтрации грунтовых вод для класса гидротехнических земляных сооружений / С.А. Положаенко. // Вісник Одеської державної академії будівництва та архітектури. — Одеса: ОДАБА, 2005.— С. 206 — 211.
3. Васильев, Ф. П. Методы решения экстремальных задач. М.: Наука, 1981.— 400 с.

МЕТОД ВИРІШЕННЯ ЗАДАЧІ ПАРАМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ МАТЕМАТИЧНИХ МОДЕЛЕЙ ПРОЦЕСІВ ФІЛЬТРАЦІЇ АНОМАЛЬНИХ РІДИН У ПОРИСТИХ СЕРЕДОВИЩАХ

С. А. Положаєнко, А. А. Фомін

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

Виконано постановку задачі параметричної ідентифікації математичних моделей (ММ) пластових систем для функцій пористості та проникності ґрунтової породи (середовища). Запропоновано метод розв'язання задачі параметричної ідентифікації досліджуваного класу ММ, заснований на методі проекції градієнту при мінімізації квадратичного критерію якості.

Ключові слова: аномальна рідина, математична модель, параметрична ідентифікація, функціонал, критерій якості, метод проекції градієнта

МЕТОД РЕШЕНИЯ ЗАДАЧИ ПАРАМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ПРОЦЕССОВ ФИЛЬТРАЦИИ АНОМАЛЬНЫХ ЖИДКОСТЕЙ В ПОРИСТЫХ СРЕДАХ

С. А. Положаенко, А. А. Фомин

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

Выполнена постановка задачи параметрической идентификации математических моделей (ММ) пластовых систем для функций пористости и проницаемости грунтовой породы (среды). Предложен метод решения задачи параметрической идентификации исследуемого класса ММ, основанный на методе проекции градиента при минимизации квадратичного критерия качества.

Ключевые слова: аномальная жидкость, математическая модель, параметрическая идентификация, функционал, критерий качества, метод проекции градиента

УДК 681.3.068

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 3, pp. 225-232

НЕЧЕТКО-ВЕРОЯТНОСТНАЯ МОДЕЛЬ ОЦЕНОК РИСКОВ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ

Н.Д. Рудниченко, В.В. Вычужанин

Одесский национальный морской университет,
Мечникова 34, Одесса,65029, Украина, e-mail: murder8910@mail.ru

В статье приведены результаты исследований разработанной нечетко-вероятностной модели оценок рисков сложных технических систем. Разработаны алгоритм нечеткого логического вывода и схематическая структура нечетко-вероятностной модели оценок рисков сложных технических систем. Сформирована база правил нечетких продукций для предложенных лингвистических переменных нечетко-вероятностной модели оценок рисков. На основании полученных результатов исследований построена трехмерная визуализация поверхности нечетко-вероятностной модели оценки структурного и функционального риска элементов и межэлементных связей судовой энергетической установки. Результаты исследования разработанной нечетко-вероятностной модели оценки риска судовой энергетической установки позволили оценить влияние ущерба и вероятности выхода из строя элементов и межэлементных связей на общий уровень риска судовой энергетической установки. Полученные результаты исследований и разработок позволяют повысить эффективность эксплуатации сложных технических систем, обеспечить качественное прогнозирование надежности их функционирования в аварийных экстремальных ситуациях.

Ключевые слова: нечеткое моделирование, сложные технические системы, оценка рисков, нечеткая логика, нечетко-вероятностная модель.

Введение

Многообразие методов оценки рисков сложных технических систем (СТС) базируется на инженерных, модельных, экспертных и других подходах [1, 2 – 4]. Подобные методы связаны со сложными расчетами, определяющими значения оценок рисков с точностью не выше первого порядка. В работах [3, 5 - 7] для обеспечения безопасности СТС рекомендуется пользоваться данными, полученными сочетанием качественных и количественных методов оценок рисков. Это позволяет осуществить анализ рисков СТС при использовании меньшего объема информации и затрат труда. Однако авторы оценки рисков СТС для автоматизации принятия решений в аварийных сценариях осуществляют без подхода, основанного на учете взаимосвязанности и взаимодействия их структурных компонентов, состоящих из элементов и межэлементных связей (МС). Учитывая объективно существующую неопределенность, неполноту и нечеткость информации при оценке рисков СТС как сложных комплексов функционально взаимосвязанных структурных компонентов, целесообразно использовать аппарат нечеткой логики, в том числе нечетко-вероятностную модель оценки риска СТС. Для построения нечетко-вероятностной модели оценки риска СТС в качестве входных параметров могут быть использованы ущерб при аварийных сценариях и их вероятность.

Цель статьи и постановка задачи исследований

Целью работы является исследование нечетко-вероятностной модели оценок рисков сложных технических систем в аварийных сценариях с учетом взаимосвязанности и взаимодействия их элементов и межэлементных связей.

Для достижения поставленной цели необходимо разработать нечетко-вероятностную модель оценок рисков сложных технических систем.

Основная часть

Построение нечетко-вероятностной модели оценки структурного риска элементов и межэлементных связей СТС осуществлено с помощью пакета прикладных программ Matlab, графических средств и инструментов пакета расширения Matlab – Fuzzy Logic Toolbox [8]. Оценка рисков на основе нечеткой логики проводилась в соответствии с алгоритмом нечеткого логического вывода по базе правил Мамдани, представляющего собой композицию с использованием операции максимум (max). Это позволяет получить итоговое нечеткое подмножество для выходной переменной с функцией принадлежности вида (1)

$$\mu_{\Sigma}(y_R) = \mu_{xi}(y_R) = \max_{y_R}[\mu_{x_{P_i}}(y_R), \mu_{x_{Y_i}}(y_R)], \qquad (1)$$

где $\mu_{\Sigma}(y_R)$ – итоговое нечеткое подмножество для выходной переменной риска (y_R);

$\mu_{xi}(y_R)$ – нечеткие множества, входящие в состав подмножества $\mu_{\Sigma}(y_R)$;

$\mu_{x_{P_i}}(y_R)$ – нечеткое множество вероятностей выхода из строя элементов и МС СЭУ;

$\mu_{x_{Y_i}}(y_R)$ – нечеткое множество ущербов элементов и МС СЭУ.

Ввод продукционных правил осуществлялся на основании обобщенной функции желательности Харрингтона для разработанного метода оценок рисков [9]. В качестве функции принадлежности использовалась функция распределения Гаусса, реализованная в Matlab в виде gaussmf для задания гладких симметричных функций принадлежности. На этапе фазификации задавались входные переменные нечетко-вероятностной модели оценки риска СТС в виде вероятностей выхода из строя и ущербов их по элементам и МС. Значения функций принадлежности по лингвистическим термам приведены в таблице 1.

Реализация операции агрегирования основывалась на методе максимизации, реализованном в Matlab в виде max. При активизации заключений весовые значения для всех входных переменных нечетко-вероятностной модели были приняты равными единице. При аккумуляции для объединения всех степеней истинности заключений правил использовался метод max-дизъюнкции. Формирование базы правил проводилось на основании нечетких продукций в форме «если–то» и функций принадлежности для соответствующих логических термов. Разработанная нечетко-вероятностная модель оценки рисков СТС, на примере судовой энергетической установки (СЭУ) с учетом [10] содержит 25 логических правил (таблица 2). Фрагмент базы логических правил нечетко-вероятностной модели оценки структурного и функционального рисков элементов и МС СЭУ в виде нечетких продукций в Rule Editor приведен на рис. 1.

Таблица 1.

Лингвистические переменные и их функции принадлежности

Название лингвистической переменной	Термы переменной (символьный вид)	Область определения функции принадлежности
Ущерб (Y)	Незначительный	x , 0, 0.25
	Низкий	x , 0.125, 0.38
	Средний	x , 0.25, 0.65
	Высокий	x , 0.55, 0.82
	Критический	x , 0.75, 1
Вероятность выхода из строя (P)	Незначительная	x , 0, 0.15
	Низкая	x , 0.1, 0.35
	Средняя	x , 0.25, 0.6
	Высокая	x , 0.45, 0.75
	Критическая	x , 0.6, 1
Риск (R)	Минимальный	y , 0, 0.25
	Допустимый	y , 0.125, 0.38
	Максимальный	y , 0.25, 0.65
	Критический	y , 0.75, 1

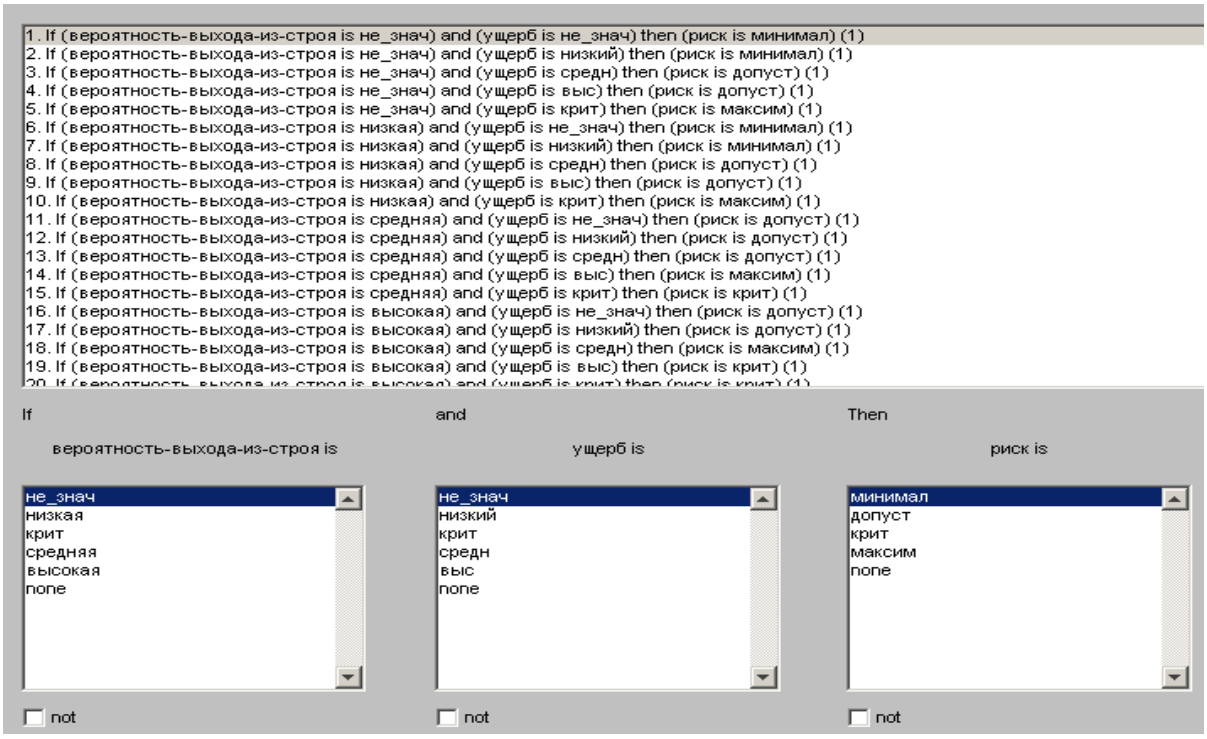


Рис 1. Фрагмент базы логических правил нечетко-вероятностной модели

Таблица 2.

База правил нечетких продукций

Имя переменной	Номер правила			
	1	2	3	4
x_P	незначительная	незначительная	незначительная	незначительная
x_Y	незначительный	незначительный	средний	высокий
y_R	минимальный	минимальный	допустимый	допустимый
Имя переменной	Номер правила			
	5	6	7	8
x_P	незначительная	низкая	низкая	низкая
x_Y	критический	незначительный	низкий	средний
y_R	максимальный	минимальный	минимальный	допустимый
Имя переменной	Номер правила			
	9	10	11	12
x_P	низкая	низкая	средняя	средняя
x_Y	высокий	критический	незначительный	низкий
y_R	допустимый	максимальный	допустимый	допустимый
Имя переменной	Номер правила			
	13	14	15	16
x_P	средняя	средняя	средняя	высокая
x_Y	средний	высокий	критический	незначительный
y_R	максимальный	максимальный	критический	допустимый
Имя переменной	Номер правила			
	17	18	19	20
x_P	высокая	высокая	высокая	высокая
x_Y	низкий	средний	высокий	критический
y_R	допустимый	максимальный	критический	критический
Имя переменной	Номер правила			
	21	22	23	24
x_P	критическая	критическая	критическая	критическая
x_Y	незначительный	низкий	средний	высокий
y_R	максимальный	максимальный	критический	критический
Имя переменной	Номер правила			
	25			
x_P	критическая			
x_Y	критический			
y_R	критический			

Дефазификация проведена с помощью реализованного в Matlab метода центра тяжести согласно (2).

$$\overline{y_R} = \int_{\min}^{\max} y_R \cdot \mu(y_R) dy_R, \int_{\min}^{\max} \mu(y_R) dy_R, \qquad (2)$$

где $\overline{y_R}$ – результат дефазификации; y_R – переменная, соответствующая выходной лингвистической переменной R; $\mu(y_R)$ – функция принадлежности нечеткого множества, соответствующего выходной переменной R после этапа аккумуляции; min и max – левая и правая точки интервала носителя нечеткого множества рассматриваемой выходной переменной R.

Ущерб для элементов и МС СЭУ задавался с использованием лингвистических переменных «Незначительный» (0-0.25), «Низкий» (0.12-0.36), «Средний» (0.3-0.6), «Высокий» (0.55-0.8), «Критический» (0.7-1). Вероятность выхода из строя элементов и МС СЭУ задавалась с использованием лингвистических переменных «Незначительная» (0-0.15), «Низкая» (0.1-0.31), «Средняя» (0.22-0.6), «Высокая» (0.45-0.75), «Критическая» (0.6-1). В качестве лингвистических переменных при построении нечетко-вероятностной модели оценки структурного риска элементов и МС СЭУ использовались термины «Минимальный риск» (0-0.2), «Допустимый риск» (0.1-0.35), «Значительный риск» (0.3-0.65), «Критический риск» (0.63-1).

Для моделирования и формализации представления критериев риска СЭУ получена трехмерная визуализация поверхности разработанной нечетко-вероятностной модели оценки риска элементов и МС СЭУ (рис. 2).

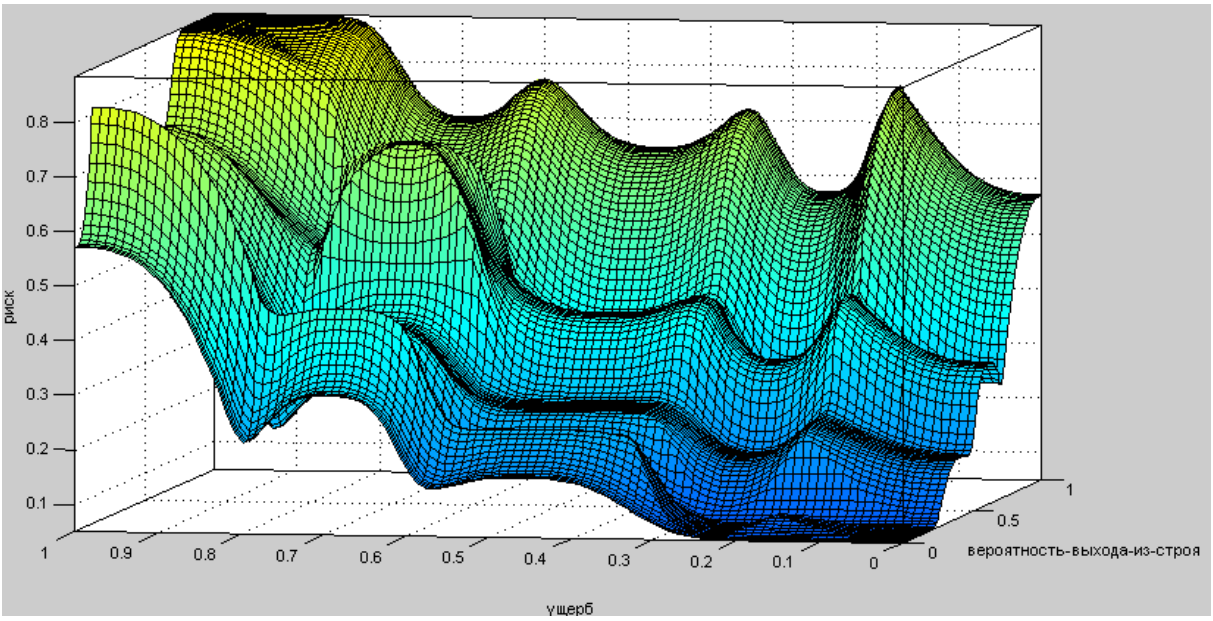


Рис 2. Трехмерная визуализация поверхности нечетко-вероятностной модели оценки структурного и функционального риска элементов и МС СЭУ

На оси абсцисс отложены значения вероятностей выхода из строя элементов и МС СЭУ, на оси ординат – значения рисков элементов и МС СЭУ, ось аппликат содержит значения рисков элементов и МС СЭУ. Разработанная нечетко-вероятностная модель позволяет получить значения рисков для каждой точки, принадлежащей трехмерной поверхности, а также отражает качественные переходы между значениями параметров в виде «впадин» и «всплесков».

Визуализация нечеткого логического вывода правил нечетко-вероятностной модели оценки структурного и функционального риска элементов и МС СЭУ приведена на рис. 3.

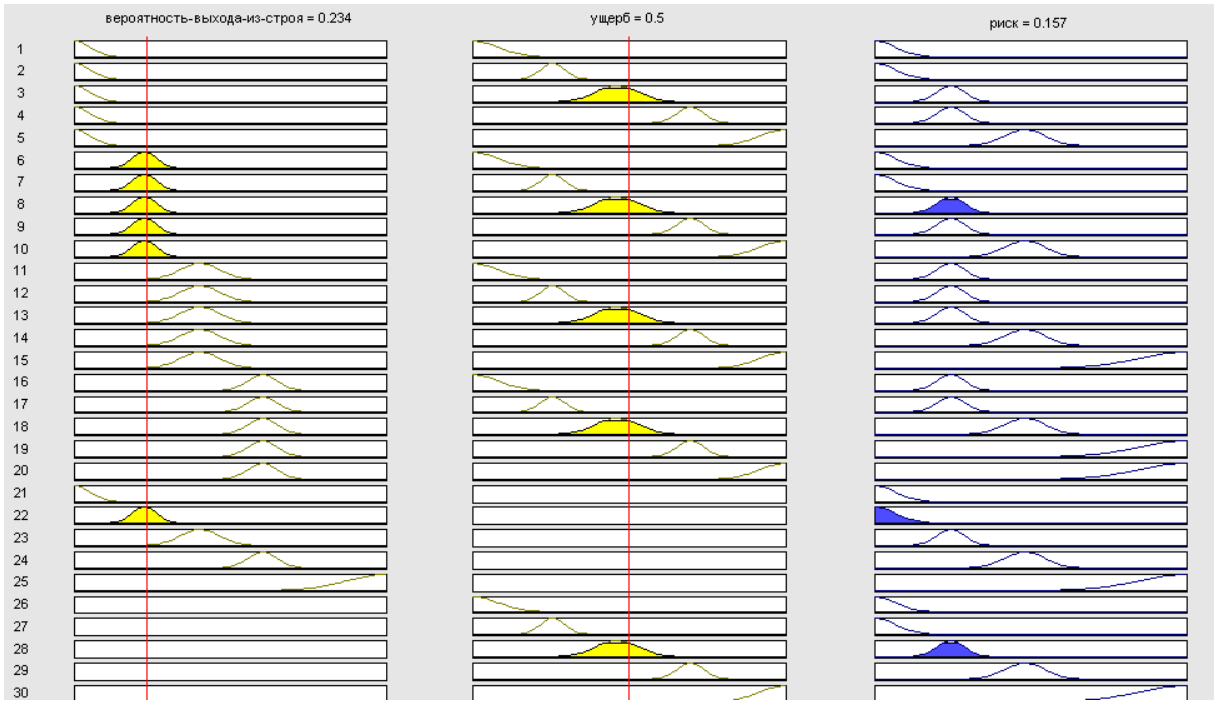


Рис. 3. Правила нечетко-вероятностной модели оценок рисков СЭУ

Визуализация осуществлена с помощью GUI-модуля Rule Viewer пакета Fuzzy Logic Toolbox, позволяющего проиллюстрировать ход логического вывода по каждому правилу, получение результирующего нечеткого множества и выполнение процедуры дефазификации функционального риска элементов и МС СЭУ.

Проверка разработанной нечетко-вероятностной модели оценки структурного и функционального риска элементов и МС СЭУ с помощью задания различных правил (рис.3) была выполнена для ряда значений входных и выходных переменных. В частности, при значениях ущерба равного 0.234 и вероятности выхода из строя равной 0.5, значение выходной переменной – риска составило 0.157, т.е. порядка 16%. Такие данные свидетельствуют о том, что имеет место невысокая степень опасности нарушения работоспособности СЭУ. Согласно полученной трехмерной визуализации поверхности нечетко-вероятностной модели оценки наибольший рост уровня риска СЭУ наблюдается при значениях вероятности выхода из строя в диапазоне 0.5… 1.

Выводы

Применение разработанной нечетко-вероятностной модели оценки рисков проектируемых и эксплуатируемых СТС с учетом вариационной информации об оценках рисков в различных сценариях изменений ущербов и вероятностей выхода из строя элементов и МС СТС обеспечивает исследование моделей систем в аварийных сценариях с учетом взаимосвязанности и взаимодействия их элементов и межэлементных связей.

Список литературы

1. Рябинин, И. А. Надежность и безопасность структурно-сложных систем / И. А. Рябинин. – СПб.: Изд-во С.-Петерб. ун-та, 2007. – 276 с.
2. Klein, J. H. An approach to technical risk assessment / J. H. Klein, R. B. Cork // International Journal of Project Management. – 1998. – 16 (6). – P. 345-351
3. Rausand, M. System Reliability Theory: Models, Statistical Methods, and Applications, Second Edition / M. Rausand, A. Hoyland. – Wiley-Interscience, 2003. – 351 p.
4. Covello, V. T. Risk Assessment Methods. Approaches for Assessing Health and Environmental Risks / V. T. Covello, M. W. Merkhofer. – Plenum Press, New York and London, 1993. – 319 p.
5. O'Neill, John. Technical Risk Assessment: a Practitioner's Guide / John O'Neill, Nitin Thakur, Alan Duus. – Australia, 2007. – 29 p.
6. Henley Ernest, J. Reliability engineering and risk assessment. / J. Ernest Henley, Hiromitsu Kumamoto. – New York : IEEE Press, Prentice-Hall, Inc., Englewood Cliffs, N.J. - 1992. – 568 p.
7. Kertzner, P. Process Control System Security Technical Risk Assessment Methodology & Technical Implementation / P. Kertzner, J.Watters, D.Bodeau // Research Report. – 2008. – № 13. – 47 p.
8. Леоненков, А. Нечеткое моделирование в среде MATLAB и fuzzyTECH. – СПб.: БХВ-Петербург, 2005. – 736 с.
9. Рудниченко, Н. Информационная когнитивная модель технологической взаимозависимости сложных технических систем / Н. Д. Рудниченко, В. В. Вычужанин // Информатика и математические методы в моделировании. – 2013. – №3. – С. 240-247.
10. Покусаев, М.Н. Система диагностики судовых энергетических установок с применением нейросетевых моделей / М.Н. Покусаев, Н.Н. Касимов // Вестник АГТУ, Управление вычислительная техника и информатика. – 2012. – №2. – С. 88-92.

НЕЧІТКО-ЙМОВІРНІСНА МОДЕЛЬ ОЦІНОК РИЗИКІВ СКЛАДНИХ ТЕХНІЧНИХ СИСТЕМ

Н.Д. Рудніченко, В.В. Вичужанін

Одеський національний морський університет,
Мечникова 34, Одеса, 65404, Україна, e-mail: murder8910@mail.ru

У статті наведено результати досліджень розробленої нечітко - імовірнісної моделі оцінок ризиків складних технічних систем. Розроблено алгоритм нечіткого логічного висновку і схематичну структуру нечітко - імовірнісної моделі оцінок ризиків складних технічних систем. Сформовано базу правил нечітких продукцій для запропонованих лінгвістичних змінних нечітко - імовірнісної моделі оцінок ризиків. На підставі отриманих результатів досліджень побудована тривимірна візуалізація поверхні нечітко - імовірнісної моделі оцінки структурного та функціонального ризику елементів і міжелементних зв'язків складної технічної системи. Результати дослідження розробленої нечітко - імовірнісної моделі оцінки ризику складної технічної системи дозволили оцінити вплив збитку і ймовірності виходу з ладу елементів і міжелементних зв'язків на загальний рівень ризику складної технічної системи. Отримані результати досліджень і розробок дозволяють підвищити ефективність експлуатації складних технічних систем, забезпечити якісне прогнозування надійності їх функціонування у різних сценаріях розвитку аварійних ситуацій.

Ключові слова: нечітке моделювання, складні технічні системи, оцінка ризиків, нечітка логіка, нечітко - імовірнісна модель.

FUZZY-PROBABILITY MODEL FOR ASSESSING THE RISKS IN COMPLEX TECHNICAL SYSTEMS

N.D. Rudnichenko, V.V. Vychuzhanin

Odesa National Marine University,
34 Mechnikov Str., 65404, Ukraine; e-mail: murder8910@mail.ru

In this paper, the authors present the results of their research of a fuzzy-probability model developed for assessing the risks in complex technical systems. A fuzzy inference algorithm and a schematic structure for the fuzzy-probability model assessing the risks in complex technical systems were developed. A fuzzy production rulebase was formed for the linguistic variables proposed for the fuzzy-probability model developed for assessing the risks. Based on the research results, the authors developed a 3-D visualization for the surface of fuzzy-probability model for assessing the structural and functional risks of the elements and element-to-element links in a complex technical system. The results of research of the fuzzy-probability model developed for assessing the risks in complex technical systems made it possible to assess the effect of damage and failure probability of the elements and element-to-element links on a total risk level of a complex technical system. The research and development results obtained make it possible to improve the efficiency of operation of complex technical systems and to give a high-quality forecast of their operational reliability under various emergency scenarios.

Keywords: fuzzy modeling, complex technical systems, risk assessment, fuzzy logic, fuzzy-probability model.

УДК 519.852: 004.424.27.021

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 3, pp. 233-238

МОДИФИКАЦИЯ МЕТОДА ВЕТВЕЙ И ГРАНИЦ ДЛЯ РЕШЕНИЯ ЗАДАЧИ РАЗМЕЩЕНИЯ ПРОИЗВОДИТЕЛЬНЫХ СИЛ

Б.И. Юхименко

Одесский национальный политехнический университет
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: pm1987pm@gmail.com

В работе приведена модификация метода ветвей и границ для решения задачи размещения производительных сил для случая, когда выбираем экономически выгодный объем производства и приведенных возможных объемов. Заслуживает внимание способ получения исходного варианта решения, а также способ оценивания подмножеств вариантов.

Ключевые слова: мощность, размещение, метод, алгоритм, скорость сходимости.

Введение

Одной из актуальных проблем в организационном управлении является проблема размещения производительных сил. Определение оптимальных объемов производства, а зачастую и места их размещения, связано с решением ряда экономических и математических задач. Решение этих задач возможно лишь при помощи математических методов и компьютерных технологий, применяемых в последнее время во многих жизнедеятельных ситуациях.

В работе [1] приведен ряд модулей математического описания задачи размещения производительных сил. Конкретная математическая модель может быть собрана из этих модулей в зависимости от того, что считается критерием оптимизации, и какая информация представляется о возможных пунктах и объемах производства в каждом. Следуя приведенной систематизации проблемы, можно построить не одну математическую модель, адекватно описывающую задачу размещения производительных сил, учитывая мотивацию решаемой проблемы, цели и условия размещения.

Цель статьи и постановка заданий

Методы реализации моделей зависят от класса задач оптимизации, которому относится полученная модель. Чаще всего классические методы не приспособлены для конкретной модели, а в некоторых случаях практически нереализуемы.

В данной работе приводится описание модифицированного алгоритма метода ветвей и границ, реализующего модель задачи размещения производительных сил, как задачи частично целочисленного линейного программирования с булевыми переменными.

Актуальность и новизна разработки заключается в том, что для конкретной модели разработан уникальный алгоритм, легко реализуемый в среде пакета Matlab [2].

Основная часть

Рассматривается случай размещения производительных сил, когда критерием оптимизации являются суммарные затраты на строительство или реконструкцию предприятий производителей, производственные расходы, определяемые с учетом объемов производства, и транспортные расходы на доставку готовой продукции для полного удовлетворения спроса потребителей. Считается известными возможные пункты производства, их месторасположения и для каждого пункта даётся перечень объемов производства, один из которых может быть выбран, как самый выгодный. Введем обозначения. Имеем:

- m возможных экономически обоснованных пунктов производства $i = \overline{1,m}$;
- в каждом i-ом пункте производства можно выбрать один объем из заданного списка a_i^k ($k = \overline{1,p_i}$; p_i - длина списка в i-ом пункте);
- n пунктов потребления $j = \overline{1,n}$;
- в каждом j-ом пункте потребления объем потребности заранее известен, обозначим через b_j;
- $\|c_{ij}\|_{i=\overline{1,m};\, j=\overline{1,n}}$ транспортные расходы на перевозку единицы продукции из каждого возможного пункта производства в каждый пункт потребления;
- k_i^k и $s_i^k \cdot a_i^k$ величина капиталовложений и производственные расходы соответственно объему производства (s_i^k - себестоимость единицы продукции при объеме производства a_i^k).

Искомые величины, необходимые для формального представления математической модели, двух типов:

- непрерывные x_{ij}, означающие объемы перевозок из любого пункта производства в любой пункт потребления ($i = \overline{1,m}$; $j = \overline{1,n}$);
- булевые переменные y_i^k для математического представления комбинаторной процедуры выбора объема производства из списка.

При перечисленных условиях и согласно введенным обозначениям математическая модель имеет вид

$$Z = \min\left\{\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}x_{ij} + \sum_{i=1}^{m}\sum_{k=1}^{P_i} s_i^k a_i^k y_i^k + E\sum_{i=1}^{m}\sum_{k=1}^{P_i} k_i^k y_i^k\right\}, \quad (1)$$

где E – коэффициент эффективности капитальных вложений.

При ограничениях

$$\sum_{j=1}^{n} x_{ij} \le \sum_{k=1}^{P_i} a_i^k y_i^k, i = \overline{1,m}; \quad (2)$$

$$\sum_{i=1}^{m} x_{ij} = b_j, j = \overline{1,n};$$

$$\sum_{i=1}^{m} b_{j,} j = \overline{1,n}; \quad (3)$$

$$\sum_{k=1}^{Pi} y_i^k = 1, i = \overline{1,m}; \quad (4)$$

$$x_{ij} \geq 0, i = \overline{1,m}; j = \overline{1,n}; \quad (5)$$

$$y_i^k \in \{0,1\}, i = \overline{1,m}; k = \overline{1,p_i}. \quad (6)$$

Правые части ограничений (2) совместно с ограничениями (4) и дополнительными требованиями искомым величинам y_i^k (требование (6)) предопределяют объем производства в пункте производства, которого обозначили через i. Через те же булевые переменные y_i^k записывается величина капиталовложений и производственные затраты, входящие части в целевой функции.

Модель (1)-(6) представляет задачу частично целочисленного линейного программирования, имеет конечное число решений по отношению к переменным y_i^k и может решаться методом ветвей и границ [3]. Метод является переборным методом, относится к классу NP полных алгоритмических проблем. Успешность метода зависит от алгоритмического способа получения оценок множества вариантов и способа разбиения множества на подмножества. Общая методика алгоритмизации метода заключается в расширении-сужении множества вариантов с целью приведения модели задачи к легкореализуемой математической модели. К примеру, для получения оценки множества вариантов задачи целочисленного линейного программирования решается соответствующая задача линейного программирования. Что касается вопроса разбиения конечного множества вариантов на подмножества, то используется идея последовательного построения решения [4]. Последовательная конкретизация значений компонент вектора решений предопределяет подмножество вариантов с конкретными значениями отдельных компонентов. К примеру, если конкретизируется компонента, скажем x_5, то множества вариантов разбивается на два подмножества (случай задачи с булевыми переменными). Одно подмножество содержит все варианты со значением компонента $x_5 = 1$, а второе – все варианты с $x_5 = 0$.

Признак оптимальности метода ветвей и границ призван не только для проверки на оптимальность найденного варианта решения, но и для уменьшения количества пересматриваемых вариантов. В принципе он не зависит от алгоритмического способа оценивания множества вариантов, но его эффективность в смысле отбрасывания не перспективных вариантов зависит от точности получаемых оценок, т.е. от уровня приближенности оценки подмножества вариантов от значений целевой функции его вариантов.

В случае алгоритмизации метода ветвей и границ для реализации модели (1) - (6) множество вариантов решения будут вектора $X = \{x_1, x_2, ..., x_m\}$, размерность которых (число m) определяется количеством предприятий-производителей, а значения – это выбираемые объемы производства из соответствующих по номеру списков объемов. Вариант решения задачи размещения формируется последовательно, переходя от одного предприятия к другому, выбирая при этом предпочтительный объем производства для каждого предприятия.

Дерево решений интерпретирует последовательное построение решения. На каждом ярусе дерева перечисляются значения конкретизируемой переменной, соответствующие объему производства согласно списку. Для дальнейшего ветвления выбирается вершина на ярусе, которая соответствует предпочтительному объему производства для данного предприятия.

Например. Пусть рассматриваются три предприятия производителя со списком объемов производства a_1^1, a_1^2, a_1^3; a_2^1, a_2^2 и $a_3^1, a_3^2, a_3^3, a_3^4$. Дерево решений для получения одного варианта приведено на рис 1.

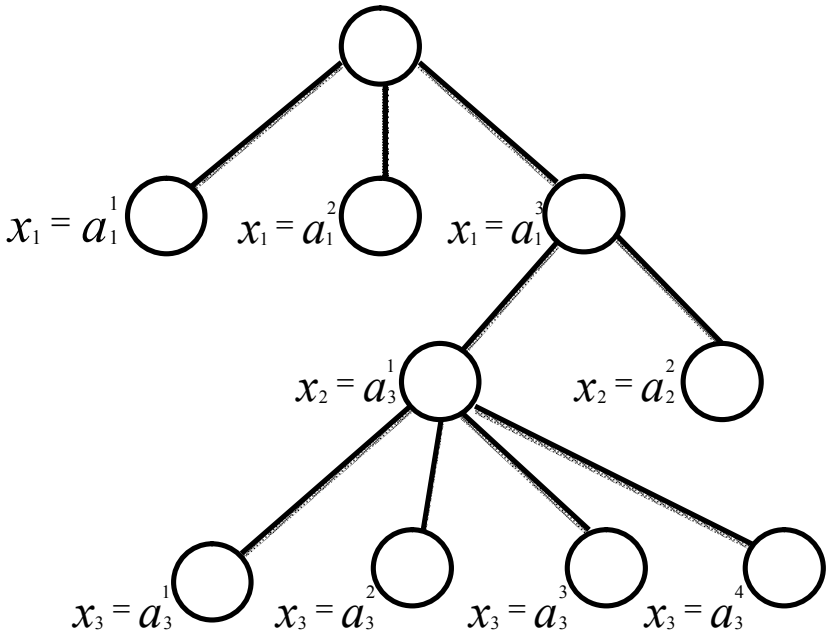


Рис. 1. Дерево решений

На первом ярусе интуитивно приняли предпочтительным объемом производства a_1^3, на втором - a_2^1 и на третьем скажем a_3^3. Вариант решения в таком случае будет вектор $X = \left(a_1^3, a_2^1, a_3^3\right)$.

Предпочтение отдается объему, для которого суммарные расходы минимальные. Расходы состоят из капиталовложений и производственных, соответствующих оцениваемому объему на конкретном ярусе. Транспортные расходы определяются путем решения транспортной задачи, считая, что в данном пункте производства имеется оцениваемый объем производства, а для всех остальных предприятий берутся максимально возможные объемы производства.

Пусть на i_0-ом ярусе выбирается предпочтительный вариант, среди всех объемов, перечисляемых на ярусе $k = \overline{1, p_{1_0}}$.

Согласно введённым обозначениям транспортные расходы определяются путем решения транспортной задачи в постановке

$$Z_{i_0}^k = \min \sum_{j=1}^{n} c_{ij} x_{ij}$$

при ограничениях

$$\sum_{j=1}^{m} x_{ij} \le a_i^{p_i}, i = \overline{1, m}; i \ne i_0;$$

$$\sum_{j=1}^{m} x_{ij} \le a_{i_0}^{k};$$

$$\sum_{i=0}^{n} x_{ij} = b_j, j = \overline{1,m};$$

$x_{ij} \ge 0$, для всех i и j.

Если решены все транспортные задачи, когда $k = \overline{1, p_{1_0}}$ и если $Z_{i_0}^{k_0} = \min\limits_{k=1,p_{i_0}} \left\{ Z_{i_0}^{k} + K_{i_0}^{k} + S_{i_0}^{k} \cdot a_{i_0} \right\}$, то объем $a_{i_0}^{k_0}$ является предпочтительным объемом. Дальнейшему разбиению подлежит подмножество вариантов, содержащее $x_{i_0} = a_{i_0}^{k_0}$.

Согласно классическому методу ветвей и границ признак оптимальности формируется на основе оценок подмножеств вариантов. Кроме того, передвигаясь по дереву решений вниз, невозможно получить улучшение значения целевой функции, тем самым, и оценок подмножеств. Последовательная конкретизация значений переменных уменьшает количество вариантов в их подмножествах.

В случае алгоритмизации метода ветвей и границ для рассматриваемой задачи размещения производительных сил оценку подмножеств вариантов решения предполагается провести следующим образом.

Пусть оценивается вершина дерева r_1 на уровне r, соответствующая объему производства $a_r^{r_1}$, который не был выбран при построении варианта решения. Транспортные расходы, которые были определены при наилучших условиях, имеются, т.е. $Z_r^{r_1}$.

Производственные расходы и капиталовложения тоже подсчитаны для конкретного объема и составляют $\left(K_r^{r_1} + S_r^{r_1} \cdot a_r^{r_1} \right)$. Для остальных уровней производственные расходы и капиталовложения $i = \overline{1,m}$ и $i \ne r$ выбираются как минимальные для каждого уровня. Таким образом, оценка подмножества вариантов, которое содержит конкретизируемую переменную x_{r_1} как величину $a_r^{r_1} \left(x_{r_1} = a_r^{r_1} \right)$, определяется по формуле

$$\xi\left(a_r^{r_1}\right) = \left\{ \sum_{\substack{i=\overline{1,r} \\ i \ne r}}^{m} \min_{\substack{k=1,p_i \\ k \ne r_1}} \left(K_i^k + S_i^k \cdot a_i^k \right) + \left(K_r^{r_1} + S_r^{r_1} \cdot a_r^{r_1} + Z_r^{r_1} \right) \right\}.$$

При наличии оценок всех подмножеств, которые не входили в прохождении по дереву при определении варианта, можно проверить полученный вариант на оптимальность. Если вариант не оптимальный, то выбирается вершина, как обычно, с наилучшей оценкой.

Выводы

Приведенный алгоритм довольно эффективен в вычислительном смысле. Процедура получения оценок подмножеств вариантов практически приведена к минимальным вычислениям. Практически производится суммирование уже определенных численных величин, которые либо известны изначально, либо определены при выборе предпочтительного варианта. Также следует отметить, что

определение величины транспортных расходов на одном ярусе дерева решений может производиться не для каждого объема производства. Если конкретизируемый объем производства не является «узким» местом в ограничениях, то его увеличение не приведет к изменению суммарных транспортных расходов. Решать повторно при другом объеме производства нет необходимости. Скорость сходимости алгоритма делает его приемлемым даже при больших объемах задачи размещения производительных сил.

Алгоритм может быть улучшен в смысле скорости сходимости, если привести эффективную процедуру нумерации предприятий производителей. Экспериментально было показано [5], что выборка компонента при последовательной конкретизации компонент вектора решений в задачах целочисленного линейного программирования с булевыми переменными улучшает скорость сходимости достаточно много.

Алгоритм апробирован и будет применен для определения оптимальных мощностей атомных станций Украины.

Список литературы

1. Юхименко, Б.И. Формализация задач размещения производительных сил. / Б. И. Юхименко // Информатика и математические методы в моделировании. – 2012. – С. 337-343.
2. Чен, К. Matlab в математических исследованиях / К. Чен, П. Джимблин, А. Ирвинг – М.: Мир, 2001. – 346 с.
3. Корбут, А. А. Дискретное программирование / А. А. Корбут, Ю. Ю. Финкельштейн. – М.: Наука, 1969. – 320 с.
4. Михалевич, В. С. Последовательные алгоритмы оптимизации и их применение. / В.С. Михалевич // Кибернетика. – 1965. - №1. – С. 45-55; №2 – С. 85-88.
5. Юхименко, Б. И. Сравнительная характеристика алгоритмов метода ветвей и границ для решения задач целочисленного линейного программирования / Б. И. Юхименко, Ю. Ю. Козина // Труды Одесского политехнического университета. – 2005. – вып. 2 – С. 199-204.

МОДИФІКАЦІЯ МЕТОДУ ГІЛОК І МЕЖ ДЛЯ ВИРІШЕННЯ ЗАДАЧІ РОЗМІЩЕННЯ ПРОДУКТИВНИХ СИЛ

Б. І. Юхименко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: pm1987pm@gmail.com

У роботі наведена модифікація методу гілок і меж для вирішення задачі розміщення продуктивних сил для випадку, коли вибираємо економічно вигідний обсяг виробництва і наведених можливих обсягів. Заслуговує уваги спосіб отримання початкового варіанту рішення, а також спосіб оцінювання підмножин варіантів.

Ключові слова: потужність, розміщення, метод, алгоритм, швидкість збіжності

MODIFICATION OF A BRANCH AND BOUND METHOD FOR SOLVING THE PROBLEM OF PLACEMENT OF PRODUCTIVE RESOURCES

B.I. Yukhimenko

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: pm1987pm@gmail.com

In this paper, the authors present a modification of a branch and bound method for solving the problem of placement of productive resources for the case of selecting an economic production output from specified possible outputs. Worthy of notice are the method to obtain an initial solution as well as the method to assess the subsets of solutions.

Keywords: capacity, placement, algorithm, rate of convergence.

УДК 681.3.067

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 3, pp. 239-249

АНАЛОГОВА МОДЕЛЬ ДИНАМІКИ КОЛИВАЛЬНИХ ПРОЦЕСІВ ЗУБЧАСТОЇ ПЕРЕДАЧІ

П. В. Дяченко

Черкаський державний технологічний університет,
бул. Шевченка 460, м. Черкаси, 18006, Україна, e-mail: dpv-orion@yandex.ru

Проведено адаптацію математичної моделі динаміки коливальних процесів одноступінчастої зубчастої передачі до вигляду, зручного для застосування аналогового моделювання. Початкову математичну модель подано у вигляді системи лінійних диференціальних рівнянь другого порядку відносно узагальнених координат, визначених відповідною схемою динаміки механічної системи. Наведено вигляд базової математичної моделі з детальним описом параметрів, що її складають; показано перехід до моделі у частотному вигляді та загальну блок-схему аналогового моделювання, отриману на її основі.

Ключові слова: математична модель, аналогова модель, динаміка коливальних процесів, узагальнені координати, система диференціальних рівнянь.

Вступ

Проблема дослідження та моделювання динаміки коливальних процесів механічних систем, що містять механізми з зубчастими передачами, залишається актуальною і на сьогодні, у зв'язку зі зростаючими вимогами щодо якості таких систем. Збільшення швидкостей руху робочих органів, зниження матеріалоємності, підвищення динамічних навантажень внаслідок вібрацій і ударів, необхідність забезпечення надійної роботи обладнання та безпечних умов праці – чинники, що визначають актуальність задачі віброзахисту механічних систем.

Математичні моделі аналізу динаміки механічних систем, зазвичай являють собою системи лінійних диференціальних рівнянь, розв'язування яких, в залежності від постановки задачі та складності самої моделі, можна здійснювати використовуючи аналітичні або чисельні методи.

Динамічні процеси у механічних системах, за умови врахування великої кількості інерційно-пружних та демпфуючих параметрів, описуються у загальному випадку системами диференціальних рівнянь великої розмірності. Складність обчислень при розв'язуванні систем диференціальних рівнянь такого вигляду, застосовуючи відомі чисельні методи [3, 4], для деяких видів динамічного аналізу виявляється досить складною. До таких видів аналізу можна віднести наприклад, спектральний, або лінійний динамічний аналіз перехідних процесів у механічній системі. Одним з ефективних способів реалізації математичної моделі при дослідженні динаміки механічних систем, окрім аналітичного та чисельного, є спосіб що ґрунтується на використанні аналогового (електронного) моделювання [1]. Переваги такого способу моделювання порівняно з іншими стають очевидними при моделюванні різноманітних режимів динамічної навантаженості зубчастої передачі (наприклад, аналізу реакції передачі на зовнішній вплив, залежний від часу).

Електронне моделювання процесу полягає у його відтворенні на електронній моделі, що дає можливість дослідити як поведінку окремих елементів механічної системи, так і систему в цілому. Порівняно з іншими видами моделювання, аналогове

має ряд характерних властивостей та переваг, таких як висока швидкодія, робота у реальному часі, зручна і наочна форма введення-виведення даних, простота набору і програмування задачі, можливість під'єднання до складу моделюючого комплексу широкого набору приладів, власна безінерційність розв'язуючих елементів, відсутність впливу власних характеристик розв'язуючих елементів моделі на результати досліджень, можливість відтворення типових нелінійностей і шматково-лінійної апроксимації складних нелінійних залежностей, можливість спостерігати на екрані осцилографа коливання або реєструвати їх на вході будь-якого елемента системи і на його виході.

Існують два основних способи аналогового моделювання – за диференціальними рівняннями та за структурними схемами [6]. При постановці задачі аналогового моделювання обирається відповідний спосіб та складається схема моделювання, що являє собою електричне з'єднання типових функціонально-розв'язуючих елементів (головним чином операційних підсилювачів, перемножувачів, суматорів, інтеграторів).

Мета статті та постановка задачі

Метою даної статті є адаптація попередньо розробленої автором математичної моделі динаміки зубчастої передачі, для задач аналогового (електронного) моделювання протікаючих у ній коливних процесів.

Для досягнення поставленої у статті мети, розв'язуються такі *задачі*:

1. Початкова (базова) математична модель динаміки одноступінчастої евольвентної косозубої зубчастої передачі, шляхом еквівалентних перетворень приводиться до частотного вигляду;
2. На основі отриманої частотної моделі створюється загальна блок-схема аналогового моделювання, яка може бути реалізована засобами будь-якого моделюючого середовища.

Основна частина

Запропонована автором у роботі [2] математична модель динаміки одноступінчастої евольвентної косозубої зубчастої передачі, являє собою систему 14-ти лінійних диференціальних рівнянь другого порядку відносно узагальнених координат, складених на основі рівнянь Лагранжа другого роду, і має вигляд:

$$
\begin{aligned}
&1.\ J\ddot{\varphi} = -k_1(\varphi - \varphi_1) + M;\\
&2.\ J_{X1}\ddot{\varphi}_1 = k_1(\varphi - \varphi_1) - c_3(t) r_{B1} R_1;\\
&3.\ J_{X2}\ddot{\varphi}_2 = -k_2(\varphi_2 - \varphi_3) + c_3(t) r_{B2} R_2;\\
&4.\ J_3\ddot{\varphi}_3 = k_2(\varphi_2 - \varphi_3) + M_3;\\
&5.\ J_{Y1}\ddot{\phi}_1^Y = -C'_{1Z}(z_1 - l_1\phi_1^Y)l_1 + C''_{1Z}(z_1 + l_2\phi_1^Y)l_2 + c_3(t)\xi R_3;\\
&6.\ J_{Y2}\ddot{\phi}_2^Y = -C'_{2Z}(z_2 - l_1\phi_2^Y)l_1 + C''_{2Z}(z_2 + l_2\phi_2^Y)l_2 - c_3(t)\xi R_4;\\
&7.\ J_{Z1}\ddot{\phi}_1^Z = -C'_{1Y}(y_1 - l_1\phi_1^Z)l_1 + C''_{1Y}(y_1 + l_2\phi_1^Z)l_2 + c_3(t) r_{B1} tg\beta_0 R_5;
\end{aligned}
\qquad (1)
$$

$$8.\ J_{Z2}\ddot{\phi}_2^Z = -C'_{2Y}(y_2 - l_1\phi_1^Z)l_1 + C''_{2Y}(y_2 + l_2\phi_2^Z)l_2 - c_3(t)r_{B2}tg\beta_0 R_6;$$

$$9.\ m_1\ddot{x}_1 = C_{1X}x_1 + c_3(t)(tg\beta_0 + 1)R_7;$$

$$10.\ m_2\ddot{x}_2 = C_{2X}x_2 + c_3(t)(tg\beta_0 + 1)R_8;$$

$$11.\ m_1\ddot{y}_1 = C'_{1Y}(y_1 - l_1\phi_1^Z) + C''_{1Y}(y_1 + l_2\phi_1^Z) + c_3(t)R_9; \qquad (1)$$

$$12.\ m_2\ddot{y}_2 = C'_{2Y}(y_2 - l_1\phi_2^Z) + C''_{2Y}(y_2 + l_2\phi_1^Z) - c_3(t)R_{10};$$

$$13.\ m_1\ddot{z}_1 = C'_{1Z}(z_1 - l_1\phi_1^Y) + C''_{1z}(z_1 + l_2\phi_1^Y) + c_3(t)R_{11};$$

$$14.\ m_2\ddot{z}_2 = C'_{2Z}(z_2 - l_1\phi_2^Y) + C''_{2Z}(z_2 + l_2\phi_2^Y) - c_3(t)R_{12}.$$

У математичній моделі (1) враховано крутильні (радіальні), та лінійні (поперечно-осьові) коливання ділянок валів і зубчастих коліс у трьох площинах. Відповідність між рівняннями системи (1) та коливаннями, які вони описують, відображає таблиця 1, де ділянка валу 1 означає проміжок між привідним двигуном та зубчастим колесом 1, а ділянка валу 2 – між зубчастим колесом 2 та приєднаною масою зовнішнього навантаження відповідно.

Таблиця 1.

Відповідність між рівняннями системи (1) та описуваними коливаннями

№	Ліва частина рівняння	Тип коливання	Елемент коливання	Вісь
1.	$J\ddot{\varphi}$	крутильні	Ділянка валу 1	x_1
2.	$J_{X1}\ddot{\varphi}_1$		Зубчасте колесо 1	x_1
3.	$J_{X2}\ddot{\varphi}_2$		Зубчасте колесо 2	x_2
4.	$J_3\ddot{\varphi}_3$		Ділянка валу 2	x_2
5.	$J_{Y1}\ddot{\phi}_1^y$		Зубчасте колесо 1	y_1
6.	$J_{Y2}\ddot{\phi}_2^y$		Зубчасте колесо 2	y_2
7.	$J_{Z1}\ddot{\phi}_1^Z$	крутильні	Зубчасте колесо 1	z_1
8.	$J_{Z2}\ddot{\phi}_2^Z$		Зубчасте колесо 2	z_2
9.	$m_1\ddot{x}_1$	поздовжні	Зубчасте колесо 1	x_1
10.	$m_2\ddot{x}_2$		Зубчасте колесо 2	x_2
11.	$m_1\ddot{y}_1$	поперечні	Зубчасте колесо 1	y_1
12.	$m_2\ddot{y}_2$		Зубчасте колесо 2	y_2
13.	$m_1\ddot{z}_1$		Зубчасте колесо 1	z_1
14.	$m_2\ddot{z}_2$		Зубчасте колесо 2	z_2

Розв’язок системи диференціальних рівнянь (1) може бути реалізований як у часовій, так і у частотній областях, залежно від постановки задачі та застосованого

методу розв'язання. Пошук розв'язку у часовій області являє собою задачу Коші для систем диференціальних рівнянь, а у частотній – пов'язаний з розв'язуванням спектральних задач лінійної алгебри – (повна або часткова проблема власних чисел матриці) [3, 4]. У першому випадку розв'язком системи диференціальних рівнянь (1) буде побудова функцій, які виражають часову залежність змінних, що описують стан системи (фазових координат), у другому – спектр власних частот і форм коливань механічної системи. Отримані частоти власних коливань можна використовувати як інформаційні частоти для визначення резонансних зон при вібродіагностиці та оцінці якості динамічної системи засобами комп'ютерного моделювання.

Прийняті у математичній моделі (1) позначення можна умовно розділити на групи, до складу яких входять вектор узагальнених координат, конструктивні, геометричні, інерційно-пружні, демпфуючі та динамічні параметри механічної системи. Зокрема, вектор узагальнених координат містить 14 компонент і має вигляд $q = \{\varphi, \varphi_1, \varphi_2, \varphi_3, \phi_1^y, \phi_1^z, \phi_2^y, \phi_2^z, x_1, y_1, z_1, x_2, y_2, z_2\}^T$, де:

$\varphi, \varphi_1, \varphi_2, \varphi_3$ – кути повороту приєднаних мас та ділянок валів навколо осей x_1, x_2;

$\phi_1^y, \phi_1^z, \phi_2^y, \phi_2^z$ – кути повороту шестерні та колеса навколо осей y_1, y_2 та z_1, z_2;

$x_1, y_1, z_1, x_2, y_2, z_2$ – лінійні переміщення шестерні та колеса вздовж осей x, y, z.

Конструктивні та масо-жорсткісні параметри механічної системи складають:

m_1, m_2 – маси зубчастих коліс;

k_1, k_2 – крутильні жорсткості валів;

C'_{1Z}, C''_{1Z} – жорсткості опор вхідного валу по осі z;

C'_{1y}, C''_{1y} – жорсткості опор вхідного валу по осі y;

C_{x1} – жорсткість опори вхідного валу по осі x;

C'_{2Z}, C''_{2Z} – жорсткості опор вихідного валу по осі z;

C'_{2y}, C''_{2y} – жорсткості опор вхідного валу по осі y;

C_{x2} – жорсткість опори вхідного валу по осі x.

Геометричні параметри:

r_{b1}, r_{b2} – радіуси основних кіл зубчастих коліс;

ξ – поточна координата точки контакту зубців вздовж осей x;

α_t – торцевий кут зачеплення; β_0 – кут нахилу зуба;

l_1, l_2 – довжини валів; $\delta\varphi + j$ – сума похибки кроку зачеплення та бічного зазору зачеплення.

Динамічні параметри:

J, J_3 – моменти інерції приєднаних мас двигуна, та навантаження відносно осі x;

J_{x1}, J_{x2} – моменти інерції відносно осі x ділянок валів між зубчастими колесами та приєднаними масами відповідно;

J_{y1}, J_{y2} – моменти інерції зубчастих коліс відносно осі y;

J_{z1}, J_{z2} – моменти інерції зубчастих коліс відносно осі z;

M, M_3 – крутний момент двигуна, та момент опору механізму навантаження відповідно.

Демпфуючі параметри враховані у подальших модифікаціях базової математичної моделі.

Члени $R_1 - R_{12}$, що входять до системи рівнянь (1) являють собою циклічно повторювані функції, що враховують похибки зачеплення реальної зубчастої передачі, тобто зміщення точки контакту зубців по відповідних осях. Зокрема, похибки зачеплення мають вигляд:

$$R_1 = R_2 = R_7 = R_8 = (x_1 - x_2) \text{ - по осі } x;$$

$$R_5 = R_6 = R_9 = R_{10} = \frac{1}{\sin \alpha_t}\left[(y_1 - y_2) + (\phi_1^z - \phi_2^z) r_{b1} tg\beta_0\right] \text{ - по осі } y;$$

$$R_3 = R_4 = R_{11} = R_{12} = \frac{1}{\cos \alpha_t}\left[(z_1 - z_2) + (\phi_1^y - \phi_2^y)\xi\right] + r_{b1}\varphi_1 - r_{b2}\varphi_2 + tg\beta_0(x_1 - x_2) + \delta\varphi + j$$

по осі z.

Сумарна похибка зачеплення A по всіх осях буде складатись з окремих похибок по кожній осі і набуде вигляду [2]:

$$A = \frac{1}{\cos \alpha_t}\left[(z_1 - z_2) + (\phi_1^y - \phi_2^y)\xi\right] + r_{b1}\varphi_1 - r_{b2}\varphi_2 + tg\beta_0(x_1 - x_2) + \delta\varphi + j +$$
$$+ \frac{1}{\sin \alpha_t}\left[(y_1 - y_2) + (\phi_1^z - \phi_2^z) r_{b1} tg\beta_0\right] + (x_1 - x_2) =$$
$$= A\,(x_1; x_2; y_1; y_2; z_1; z_2; \phi_1^y; \phi_2^y; \phi_1^z; \phi_2^z; \varphi_1; \varphi_2; j; \delta\varphi).$$

На початковому етапі створення аналогової моделі динаміки зубчастої передачі введемо у диференціальні рівняння руху системи (1) лінійні та крутильні (радіальні) частоти, де $\omega^2 = \frac{c}{m}$ – лінійна частота, $\nu^2 = \frac{C_{кр}}{J}$ – крутильна частота, вважаючи жорсткість у цих виразах постійною. Враховуючи змінність жорсткості зачеплення в диференціальних рівняннях, подамо змінну жорсткість у вигляді $C_{Зкр}(t) = C_{Зкр}^{\max} f(t)$, де $f(t)$ – безрозмірна функція зміни крутильної жорсткості, використовуючи зв'язок між крутильними та лінійними жорсткостями $C_{Зкр}(t) = r_{b1}^2 C_З$, де під $C_{Зкр}$ та $C_З$ маються на увазі максимальні значення і вирази для частот. Введемо до розгляду частоти, які діють у системі з врахуванням характеру пружних деформацій та зміни жорсткості зачеплення $C_З(t) = C_З^*$.

Крутильні частоти коливань:

$$\nu^2 = \frac{k}{J};\ \nu_1^2 = \frac{k}{J_{x1}};\ \nu_{x1}^2 = r_{b1}^2 \frac{C_З^*}{J_{x1}};\ \nu_2^2 = \frac{k_1}{J_{x2}};\ \nu_{x2}^2 = r_{b2}^2 \frac{C_З^*}{J_{x2}};\ \nu_3^2 = \frac{k_1}{J_3};\ \nu_{y1}'^2 = l_1^2 \frac{C_{1z}'}{J_{y1}};$$

$$\nu_{y1}''^2 = l_2^2 \frac{C_{1z}''}{J_{y1}};\ \nu_{y1}^2 = r_{b1}^2 \frac{C_З^*}{J_{y1}};\ \nu_{y2}'^2 = l_1^2 \frac{C_{2z}'}{J_{y2}};\ \nu_{y2}''^2 = l_2^2 \frac{C_{2z}''}{J_{y2}};\ \nu_{y2}^2 = r_{b2}^2 \frac{C_З^*}{J_{y2}};\ \nu_{z1}'^2 = l_1^2 \frac{C_{1y}'}{J_{z1}};$$

$$\nu_{z1}''^2 = l_2^2 \frac{C_{1y}''}{J_{z1}};\ \nu_{z1}^2 = r_{b1}^2 \frac{C_З^*}{J_{z1}};\ \nu_{z2}'^2 = l_1^2 \frac{C_{2y}'}{J_{z2}};\ \nu_{z2}''^2 = l_2^2 \frac{C_{2y}''}{J_{z2}};\ \nu_{z2}^2 = r_{b2}^2 \frac{C_З^*}{J_{z2}}.$$

Лінійні частоти коливань:

$$\omega_1^2 = \frac{C_З^*}{m_1};\ \omega_{1x}^2 = \frac{C_{1x}}{m_1};\ \omega_2^2 = \frac{C_З^*}{m_2};\ \omega_{2x}^2 = \frac{C_{2x}}{m_2};\ \omega_{1y}'^2 = \frac{C_{1y}'}{m_1};\ \omega_{1y}''^2 = \frac{C_{1y}''}{m_1};\ \omega_1^2 = \frac{C_З^*}{m_1};\ \omega_{2y}'^2 = \frac{C_{2y}'}{m_2};\ \omega_{2y}''^2 = \frac{C_{2y}''}{m_2};$$

$$\omega_{1z}'^2 = \frac{C_{1z}'}{m_1};\ \omega_{1z}''^2 = \frac{C_{1z}''}{m_1};\ \omega_{2z}'^2 = \frac{C_{2z}'}{m_2};\ \omega_{2z}''^2 = \frac{C_{2z}''}{m_2}.$$

З урахуванням введених позначень, система диференціальних рівнянь (1) набуде вигляду:

$$\ddot{\varphi} = \nu^2(\varphi - \varphi_1) + \frac{M}{J};$$

$$\ddot{\varphi}_1 = -\nu^2(\varphi - \varphi_1) + \frac{k_{x1}^2}{r_{b1}} \cdot A \cdot f(t);$$

$$\ddot{\varphi}_2 = \nu_2^2(\varphi_2 - \varphi_3) + \frac{k_{x1}^2}{r_{b2}} \cdot A \cdot f(t);$$

$$\ddot{\varphi}_3 = -\nu_3^2(\varphi_2 - \varphi_3) + \frac{M_3}{J_3};$$

$$\ddot{\phi}_1^y = -\frac{\nu_{y1}'^2}{l_1}(z_1 - l_1\phi_1^y) + \frac{\nu_{y1}''^2}{l_2}(z_1 + l_2\phi_1^y) + \frac{\nu_{y1}^2}{r_{b1}^2} \cdot \xi \cdot \frac{1}{\cos\alpha_t} \cdot A \cdot f(t);$$

$$\ddot{\phi}_2^y = -\frac{\nu_{y2}'^2}{l_1}(z_2 - l_1\phi_2^y) + \frac{\nu_{y2}''^2}{l_2}(z_2 + l_2\phi_2^y) - \frac{\nu_{y2}^2}{r_{b2}^2} \cdot \xi \cdot \frac{1}{\cos\alpha_t} \cdot A \cdot f(t);$$

$$\ddot{\phi}_1^z = -\frac{\nu_{z1}'^2}{l_1}(y_1 - l_1\phi_1^z) + \frac{\nu_{z1}''^2}{l_2}(y_1 + l_2\phi_1^z) + \frac{\nu_{z1}^2}{r_{b1}^2} \cdot tg\beta_0 \cdot \frac{1}{\sin\alpha_t} \cdot A \cdot f(t); \qquad (2)$$

$$\ddot{\phi}_2^z = -\frac{\nu_{z2}'^2}{l_1}(y_2 - l_1\phi_2^z) + \frac{\nu_{z2}''^2}{l_2}(y_2 + l_2\phi_2^z) - \frac{\nu_{z2}^2}{r_{b2}^2} \cdot tg\beta_0 \cdot \frac{1}{\sin\alpha_t} \cdot A \cdot f(t);$$

$$\ddot{x}_1 = \omega_{1x}^2 x_1 + \omega_1^2 \cdot f(t) \cdot (tg\beta_0 + 1) \cdot A;$$

$$\ddot{x}_2 = \omega_{2x}^2 x_2 + \omega_2^2 \cdot f(t) \cdot (tg\beta_0 + 1) \cdot A;$$

$$\ddot{y}_1 = \omega_{1y}'^2(y_1 - l_1\phi_1^z) + \omega_{1y}''^2(y_1 + l_2\phi_1^z) + \omega_1^2 \cdot f(t) \cdot \frac{1}{\sin\alpha_t} \cdot A;$$

$$\ddot{y}_2 = \omega_{2y}'^2(y_2 - l_1\phi_2^z) + \omega_{2y}''^2(y_2 + l_2\phi_2^z) - \omega_2^2 \cdot f(t) \cdot \frac{1}{\sin\alpha_t} \cdot A;$$

$$\ddot{z}_1 = \omega_{1z}'^2(z_1 - l_1\phi_1^y) + \omega_{1z}''^2(z_1 + l_2\phi_1^y) + \omega_1^2 \cdot f(t) \cdot \frac{1}{\cos\alpha_t} \cdot A;$$

$$\ddot{z}_2 = \omega_{2z}'^2(z_2 - l_1\phi_2^y) + \omega_{2z}''^2(z_2 + l_2\phi_2^y) - \omega_2^2 \cdot f(t) \cdot \frac{1}{\cos\alpha_t} \cdot A.$$

Прийнявши позначення:

$$B_1 = \frac{1}{r_{b1}};\ B_2 = \frac{1}{r_{b2}};\ B_3 = \frac{\xi}{r_{b1}^2 \cos\alpha_t};\ B_4 = \frac{\xi}{r_{b2}^2 \cos\alpha_t};\ B_5 = \frac{tg\beta_0}{r_{b1} \sin\alpha_t};$$

$$B_6 = \frac{tg\beta_0}{r_{b2} \sin\alpha_t};\ B_7 = B_8 = tg\beta_0 + 1;\ B_9 = B_{10} = \frac{1}{\sin\alpha_t};\ B_{11} = B_{12} = \frac{1}{\cos\alpha_t},$$

отримуємо загальний вигляд частотної математичної моделі:

$$\ddot{\varphi} = \nu^2(\varphi - \varphi_1) + \frac{M}{J};$$

$$\ddot{\varphi}_1 = -\nu^2(\varphi - \varphi_1) + \nu_{x1}^2 \cdot f(t) \cdot A(x_1; x_2; y_1; y_2; z_1; z_2; \phi_1^y; \phi_2^y; \phi_1^z; \phi_2^z; \varphi_1; \varphi_2; j; \delta\varphi) \cdot B_1;$$

$$\ddot{\varphi}_2 = \nu_2^2(\varphi_2 - \varphi_3) + \nu_{x2}^2 \cdot f(t) \cdot A(x_1; x_2; y_1; y_2; z_1; z_2; \phi_1^y; \phi_2^y; \phi_1^z; \phi_2^z; \varphi_1; \varphi_2; j; \delta\varphi) \cdot B_2;$$

$$\ddot{\varphi}_3 = -\nu_3^2(\varphi_2 - \varphi_3) + \frac{M_3}{J_3};$$

$$\begin{aligned}
&\ddot{\phi}_1^y = -\frac{\nu_{y1}'^2}{l_1}(z_1 - l_1\phi_1^y) + \frac{\nu_{y1}''^2}{l_2}(z_1 + l_2\phi_1^y) + k_{y1}^2 \cdot f(t) \times \\
&\times A(x_1; x_2; y_1; y_2; z_1; z_2; \phi_1^y; \phi_2^y; \phi_1^z; \phi_2^z; \varphi_1; \varphi_2; j; \delta\varphi) \cdot B_3; \\
&\ddot{\phi}_2^y = -\frac{\nu_{y2}'^2}{l_1}(z_2 - l_1\phi_2^y) + \frac{\nu_{y2}''^2}{l_2}(z_2 + l_2\phi_2^y) - \nu_{y2}^2 \cdot f(t) \times \\
&\times A(x_1; x_2; y_1; y_2; z_1; z_2; \phi_1^y; \phi_2^y; \phi_1^z; \phi_2^z; \varphi_1; \varphi_2; j; \delta\varphi) \cdot B_4; \\
&\ddot{\phi}_1^z = -\frac{\nu_{z1}'^2}{l_1}(y_1 - l_1\phi_1^z) + \frac{\nu_{z1}''^2}{l_2}(y_1 + l_2\phi_1^z) + \nu_{z1}^2 \cdot f(t) \times \\
&\times A(x_1; x_2; y_1; y_2; z_1; z_2; \phi_1^y; \phi_2^y; \phi_1^z; \phi_2^z; \varphi_1; \varphi_2; j; \delta\varphi) \cdot B_5; \\
&\ddot{\phi}_2^z = -\frac{\nu_{z2}'^2}{l_1}(y_2 - l_1\phi_2^z) + \frac{\nu_{z2}''^2}{l_2}(y_2 + l_2\phi_2^z) - \nu_{z2}^2 \cdot f(t) \times \\
&\times A(x_1; x_2; y_1; y_2; z_1; z_2; \phi_1^y; \phi_2^y; \phi_1^z; \phi_2^z; \varphi_1; \varphi_2; j; \delta\varphi) \cdot B_6;
\end{aligned} \tag{3}$$

$$\ddot{x}_1 = \omega_{1x}^2 x_1 + \omega_1^2 \cdot f(t) \cdot A(x_1; x_2; y_1; y_2; z_1; z_2; \phi_1^y; \phi_2^y; \phi_1^z; \phi_2^z; \varphi_1; \varphi_2; j; \delta\varphi) \cdot B_7;$$

$$\ddot{x}_2 = \omega_{2x}^2 x_2 + \omega_2^2 \cdot f(t) \cdot A(x_1; x_2; y_1; y_2; z_1; z_2; \phi_1^y; \phi_2^y; \phi_1^z; \phi_2^z; \varphi_1; \varphi_2; j; \delta\varphi) \cdot B_8;$$

$$\begin{aligned}
&\ddot{y}_1 = \omega_{1y}'^2(y_1 - l_1\phi_1^z) + \omega_{1y}''^2(y_1 + l_2\phi_1^z) + \omega_1^2 \cdot f(t) \times \\
&\times A(x_1; x_2; y_1; y_2; z_1; z_2; \phi_1^y; \phi_2^y; \phi_1^z; \phi_2^z; \varphi_1; \varphi_2; j; \delta\varphi) \cdot B_9;
\end{aligned}$$

$$\begin{aligned}
&\ddot{y}_2 = \omega_{2y}'^2(y_2 - l_1\phi_2^z) + \omega_{2y}''^2(y_2 + l_2\phi_2^z) - \omega_2^2 \cdot f(t) \times \\
&\times A(x_1; x_2; y_1; y_2; z_1; z_2; \phi_1^y; \phi_2^y; \phi_1^z; \phi_2^z; \varphi_1; \varphi_2; j; \delta\varphi) \cdot B_{10};
\end{aligned}$$

$$\ddot{z}_1 = \omega_{1z}'^2(z_1 - l_1\phi_1^y) + \omega_{1z}''^2(z_1 + l_2\phi_1^y) + \omega_1^2 \cdot f(t)\times$$
$$\times A(x_1; x_2; y_1; y_2; z_1; z_2; \phi_1^y; \phi_2^y; \phi_1^z; \phi_2^z; \varphi_1; \varphi_2; j; \delta\varphi)\cdot B_{11};$$
$$\ddot{z}_2 = \omega_{2z}'^2(z_2 - l_1\phi_2^y) + \omega_{2z}''^2(z_2 + l_2\phi_2^y) - \omega_2^2 \cdot f(t)\times \quad (3)$$
$$\times A(x_1; x_2; y_1; y_2; z_1; z_2; \phi_1^y; \phi_2^y; \phi_1^z; \phi_2^z; \varphi_1; \varphi_2; j; \delta\varphi)\cdot B_{12}.$$

Таким чином отримано частотну математичну модель, яка у повній мірі охоплює фізичний процес роботи зубчастої передачі, і може бути розповсюджена як на косозубі, так і на прямозубі передачі. У останньому випадку у рівняннях системи (1), у виразах для потенціальної енергії, члени, які містять $tg\beta_0$ і враховують нахил зубців, будуть відсутні. Наведена модель враховує такі види похибок руху реальної зубчастої передачі, які виникають за рахунок:

- кутів закрутки валів приєднаних мас двигуна і робочої машини $(\varphi - \varphi_1) + (\varphi_2 - \varphi_3)$;
- непаралельності валів шестерні та колеса

$$(z_1 - l_1\phi_1^y) + (z_1 + l_2\phi_1^y) + (z_2 - l_1\phi_2^y) + (z_2 + l_2\phi_2^y);$$

- перекосу валів шестерні та колеса

$$(y_1 - l_1\phi_1^z) + (y_1 + l_2\phi_1^z) + (y_2 - l_1\phi_2^z) + (y_2 + l_2\phi_2^z);$$

- поздовжних (осьових) зміщень шестерні та колеса $x_1 + x_2$;
- похибки зачеплення (в напрямі лінії або площини зачеплення), переміщення в механічній системі мають вигляд:

$$\frac{1}{\cos\alpha_t}\left[(z_1 - z_2) + (\phi_1^y - \phi_2^y)\xi\right] + r_{b1}\varphi_1 - r_{b2}\varphi_2 + tg\beta_0(x_1 - x_2) + \delta\varphi + j + w +$$
$$+ \frac{1}{\sin\alpha_t}\left[(y_1 - y_2) + (\phi_1^z - \phi_2^z)r_{b1}tg\beta_0\right]$$

Приведемо систему (3) до вигляду, зручного для аналогового моделювання:

$$\ddot{\varphi} = \nu^2\varphi - \nu^2\varphi_1 + \frac{M}{J};$$

$$\ddot{\varphi}_1 = -\nu^2\varphi + \nu^2\varphi_1 + \frac{\nu_{x1}^2}{r_{b1}}\cdot A\cdot f(t);$$

$$\ddot{\varphi}_2 = \nu_2^2\varphi_2 - \nu_2^2\varphi_3 + \frac{\nu_{x1}^2}{r_{b2}}\cdot A\cdot f(t); \quad (4)$$

$$\ddot{\varphi}_3 = -\nu_3^2\varphi_2 + \nu_3^2\varphi_3) + \frac{M_3}{J_3};$$

$$\ddot{\phi}_1^y = (\nu_{y1}'^2 + \nu_{y1}''^2)\phi_1^y + (-\frac{\nu_{y1}'^2}{l_1} + \frac{\nu_{y1}''^2}{l_2})z_1 + \frac{\xi\nu_{y1}^2}{r_{b1}^2\cos\alpha_t}\cdot A\cdot f(t);$$

$$\ddot{\phi}_2^y = (\nu_{y2}'^2 + \nu_{y2}''^2)\phi_2^y + (-\frac{\nu_{y2}'^2}{l_1} + \frac{\nu_{y2}''^2}{l_2})z_2 - \frac{\xi\nu_{y2}^2}{r_{b2}^2\cos\alpha_t}\cdot A\cdot f(t);$$

$$\ddot{\phi}_1^z = (\nu_{z1}'^2 + \nu_{z1}''^2)\phi_1^z + (-\frac{\nu_{z1}'^2}{l_1} + \frac{\nu_{z1}''^2}{l_2})y_1 + \frac{tg\beta_0\nu_{z1}^2}{r_{b1}^2\sin\alpha_t}\cdot A\cdot f(t);$$

$$\ddot{\phi}_2^z = (\nu_{z2}'^2 + \nu_{z2}''^2)\phi_2^z + (-\frac{\nu_{z2}'^2}{l_1} + \frac{\nu_{z2}''^2}{l_2})y_1 + \frac{tg\beta_0\nu_{z2}^2}{r_{b2}^2\sin\alpha_t}\cdot A\cdot f(t);$$

$$\ddot{x}_1 = \omega_{x1}^2 x_1 + (tg\beta_0 + 1)\omega_1^2\cdot A\cdot f(t);$$

$$\ddot{x}_2 = \omega_{x2}^2 x_2 - (tg\beta_0 + 1)\omega_2^2\cdot A\cdot f(t);$$

(4)

$$\ddot{y}_1 = (\omega_{y1}'^2 + \omega_{y1}''^2)y_1 + (-\omega_{y1}'^2 l_1 + \omega_{y1}''^2 l_2)\phi_1^z + \frac{\omega_1^2}{\sin\alpha_t}\cdot A\cdot f(t);$$

$$\ddot{y}_2 = (\omega_{y2}'^2 + \omega_{y2}''^2)y_2 + (-\omega_{y2}'^2 l_1 + \omega_{y2}''^2 l_2)\phi_2^z + \frac{\omega_1^2}{\sin\alpha_t}\cdot A\cdot f(t);$$

$$\ddot{z}_1 = (\omega_{z1}'^2 + \omega_{z1}''^2)z_1 + (-\omega_{z1}'^2 l_1 + \omega_{z1}''^2 l_2)\phi_1^y + \frac{\omega_1^2}{\cos\alpha_t}\cdot A\cdot f(t);$$

$$\ddot{z}_2 = (\omega_{z2}'^2 + \omega_{z2}''^2)z_2 + (-\omega_{z2}'^2 l_1 + \omega_{z2}''^2 l_2)\phi_2^y + \frac{\omega_2^2}{\cos\alpha_t}\cdot A\cdot f(t).$$

Математичну модель (4) приймаємо за основу для складення схеми аналогового моделювання (схеми набору розв'язуючих елементів). При складанні схеми моделювання використаємо методику та символічну інтерпретацію елементів, викладену у [5, 6], згідно чого моделююча схема складається у відповідності зі структурною схемою диференціальних рівнянь, що описують динаміку усієї механічної системи. У цьому випадку структурна схема рівнянь виражає всі елементарні математичні операції і зв'язки між ними, властиві розглядуваній системі диференціальних рівнянь руху системи. Такі схеми універсальні у своєму застосуванні для механічних систем будь-якої складності, що містять механічні, електричні, гідравлічні та інші ланки.

Загальна схема аналогового моделювання досліджуваної механічної системи, що складена за розглянутими вище принципами, наведена на рис. 1.

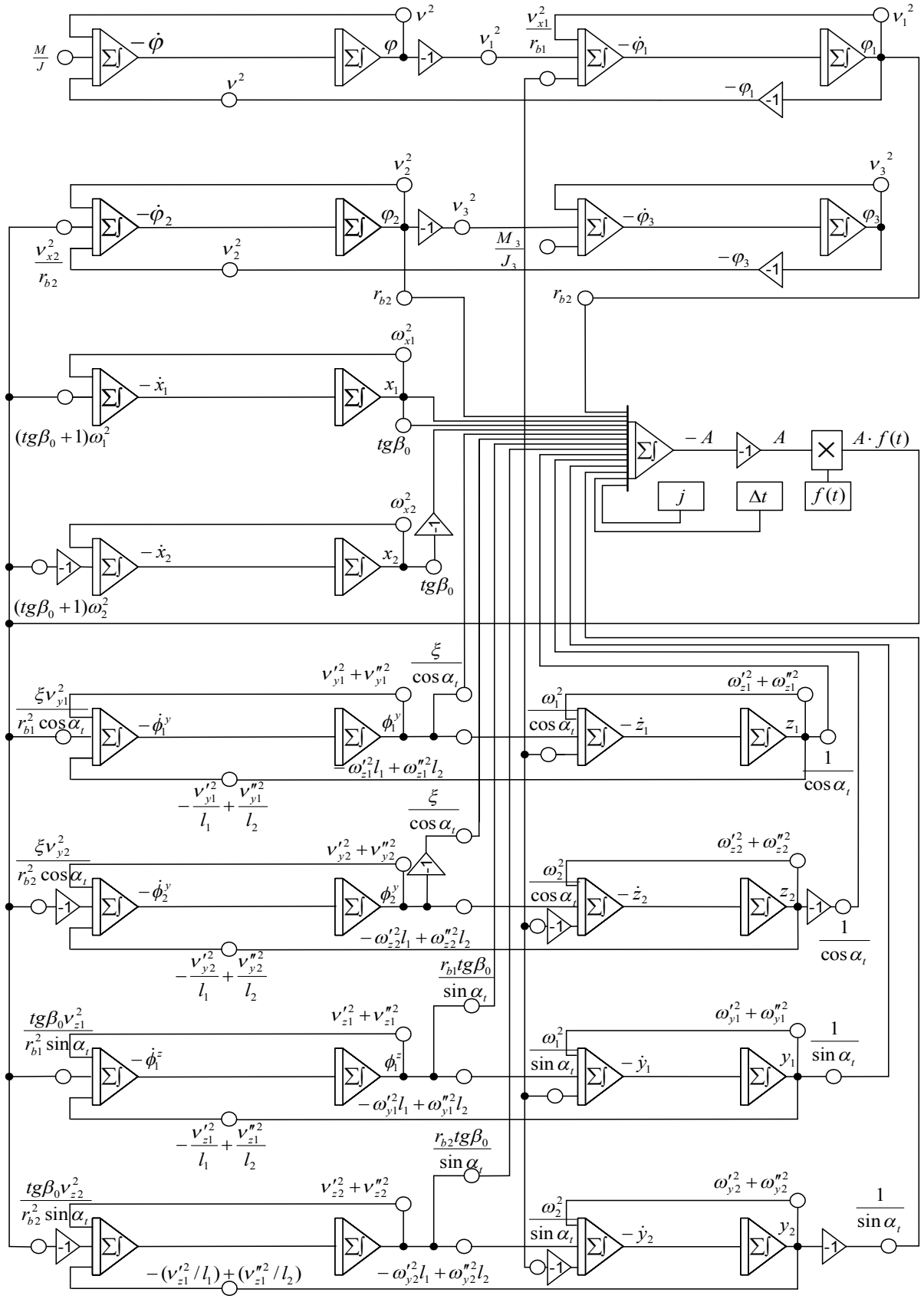


Рис. 1. Схема аналогового моделювання динаміки зубчастої передачі

Висновок

У результаті еквівалентних перетворень базової математичної моделі отримано схему аналогового моделювання динаміки одноступінчастої евольвентної косозубої зубчастої передачі. Реалізація отриманої схеми засобами моделюючого середовища Matlab-Simulink дає можливість ефективно досліджувати режими динамічної навантаженості механічної системи.

Список літератури

1. Виттенберг, И.М. Программирование аналого-цифровых вычислительных систем: Справочник / И.М. Витенберг, М.Г. Левин, И.Я. Шор // Под ред. И.М. Витенберга. – М.: Радио и связь, 1989. – 288 с.: ил.
2. Дяченко, П.В. Просторова математична модель власних частот та форм коливань механічної системи, класу одноступінчастих евольвентних зубчастих передач / П.В. Дяченко // – Донецьк: Науково-теоретичний журнал «Штучний інтелект», – 2011, №1 – ст. 54-60.
3. Демидович, Б.П. Численные методы анализа / Б.П. Демидович, И.А. Марон, Э.З. Шувалова // – М.: Физматгиз, 1963.– 400 с
4. Бахвалов, Н.С. Численные методы / Н.С. Бахвалов, И.П. Жидков, Г.М. Кобельков // – М.: Наука, 1987.–600 с.
5. Гультяев, А.И. Имитационное моделирование в среде MATLAB-5.2. Практическое пособие / А.И. Гультяев // – СПб: Корона принт. 1999, 288 с.
6. Тетельбаум, И.М. Практика аналогового моделирования динамических систем / И.М. Тетельбаум, Ю.Р. Шнейдер // Справочное пособие – М.: Энергоатомиздат, 1987. – 384 с.: ил.

АНАЛОГОВАЯ МОДЕЛЬ ДИНАМИКИ КОЛЕБАТЕЛЬНЫХ ПРОЦЕССОВ ЗУБЧАТОЙ ПЕРЕДАЧИ

П. В. Дяченко

Черкасский государственный технологический университет,
ул. Шевченко 460, г. Черкассы, 18006, Украина, e-mail: dpv-orion@yandex.ru

Проведена адаптация математической модели динамики колебательных процессов одноступенчатой зубчатой передачи, к виду, удобному для применения аналогового моделирования. Исходная математическая модель представлена в виде системы линейных дифференциальных уравнений второго порядка относительно обобщенных координат, определяемых соответствующей схемой динамики механической системы. Приведен вид базовой математической модели с подробным описанием составляющих ее параметров, показан переход к модели в частотном виде, и полученную на ее основе общую блок-схему аналогового моделирования.

Ключевые слова: математическая модель, аналоговая модель, динамика колебательных процессов, обобщенные координаты, система дифференциальных уравнений.

ANALOG MODEL OF DYNAMICS OF TOOTH GEAR OSCILLATIONS

P.V. Diachenko

Cherkasy State Technological University,
460 Shevchenko Str., Cherkasy, 18006, Ukraine; e-mail: dpv-orion@yandex.ru

A mathematical model of dynamics of tooth gear oscillation was adapted for the further use in analog modeling. An initial mathematical model was presented as a system of linear second-order differential equations referred to generalized coordinates, the latter being defined by the appropriate scheme of dynamics of mechanical system. A type of basic mathematical model was presented with the detailed description of its parameters. Additionally, a transfer to a frequency-domain model was shown, as well as a general flowchart of analog modeling obtained on its basis.

Keywords: mathematical model, analog model, dynamics of oscillations, generalized coordinates, system of differential equations.

УДК 681.513

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 3, pp. 250-255

РЕАЛИЗАЦИЯ МОДЕЛЕЙ ДИНАМИЧЕСКИХ ОБЪЕКТОВ, ПРЕДСТАВЛЕННЫХ В ВИДЕ НЕЛИНЕЙНЫХ ИНТЕГРО-ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ С КРАЕВЫМИ УСЛОВИЯМИ

Д. Э. Контрерас, С. А. Положаенко

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

Рассмотрена постановка r-точечной краевой задачи при описании динамики объектов в виде нелинейных интегро-дифференциальных уравнений. Предложен итерационный подход к решению данной задачи, основанный на методе Ньютона.

Ключевые слова: динамический объект, краевая задача, итерационный процесс, метод Ньютона, шаг дискретизации, погрешность решения

Введение

Достаточно широкий класс динамических объектов с требуемой для практики степенью адекватности может быть описан моделями в виде интегро-дифференциальных уравнений. К таким динамическим объектам, прежде всего, относятся объекты «с памятью» или «с последействием» [1]. Для случая распределенных систем интегро-дифференциальные уравнения динамики дополняются соответствующими краевыми условиями. В работе [2] показана возможность решения нелинейной *r*-точечной краевой задачи методом Ньютона на аналого-цифровых вычислительных системах. В данной работе рассматривается метод Ньютона в сочетании с квадратурно-разностными методами для решения нелинейной *r*-точечной краевой задачи в среде Matlab.

Постановка задачи

Рассмотрим r-точечную краевую задачу [2], представленную уравнением

$$L_y y = \lambda T_y y + f(t) \tag{1}$$

и краевыми нелинейными условиями

$$g\left(y(0), y(t_1), \ldots, y(t_{r-1})\right) = d\,, \tag{2}$$

где L_y – дифференциальный оператор порядка n; λ – вещественный параметр; d – n-мерный вектор;

$$T_y = \int_0^t K\left(t, s, y, y', \ldots, y^{(m)}\right) ds .$$

Решение данной задачи будем производить путем итерационного определения вектора начальных условий $y(0)$.

Нелинейная краевая задача (1) – (2) эквивалентна системе нелинейных алгебраических уравнений

$$\left.\begin{array}{l} q(y_0) = d; \\ q(y_0) = g\left[\varphi(t_0, y_0), \varphi(t_1, y_0), \ldots, \varphi(t_r, y_0)\right] \end{array}\right\} \qquad (3)$$

и задаче Коши

$$L_y y = \lambda T_y y + f(t), \; y(0) = y_0, \qquad (4)$$

где $\varphi(t, y_0)$ – решение задачи (1) в форме Коши.

Вектор начальных условий определяется из системы (3). Для решения этой системы можно применить итерационный метод Ньютона. В явном виде система (3), как правило, неизвестна, поскольку неизвестна в явном виде функция $\varphi(t, y_0)$. Однако, может быть указан алгоритм для вычисления $g(y)$ при заданном y. Итерационный процесс будет иметь следующий вид ($y^0(0)$ задается произвольно)

$$\left.\begin{array}{l} L_y y^k = \lambda T_y y^k + f(t); \\ \Gamma\left(y_0^k\right) z^k = q\left(y_0^k\right) - d; \\ y_0^{k+1} = y_0^k - z^k, \; k = 0, 1, 2, \ldots, \end{array}\right\} \qquad (5)$$

где Γ – матрица Якоби вектор-функции $g(y)$.

Описание метода решения

Процесс решения (5) заключается в следующем. Задается k-е приближение вектора начальных условий, решается задача Коши интегро-дифференциального уравнения и определяются функции $\varphi(t, y_0^k)$. Затем решается система нелинейных уравнений и определяется $k+1$ приближение вектора начальных условий.

Так как система (3) в явном виде не задана, то при практических вычислениях по методу Ньютона производные, входящие в матрицу $\Gamma\left(y^k\right)$, заменяют приближенными к ним разностями. Разностный аналог матрицы Якоби вектор-функции $g(y)$ имеет вид [2]:

$$R\left(h_k, y^k\right) = \left(\frac{g\left(y_0^k + h_k e_1\right) - g\left(y_0^k\right)}{h_k}, \ldots, \frac{g\left(y_0^k + h_k e_n\right) - g\left(y_0^k\right)}{h_k} \right),$$

где e_i – i-й координатный орт, т.е. вектор размерности n, у которого i-я компонента равна единице, а все остальные компоненты равны нулю. Для обеспечения квадратичной сходимости h_k определяется по формуле

$$h_k \le \max_i \left| g_i \left\{ \varphi\left(t_0, y_0^k\right), \varphi\left(t_1, y_0^k\right), \ldots, \varphi\left(t_{r-1}, y_0^k\right) \right\} \right|.$$

Введем обозначение $y_{t_s}^{i,k} = y^{i,k}(t_s)$, $(s = 1, \ldots r)$. Тогда вычислительная схема решения нелинейной краевой задачи примет вид [2]

$$\left.\begin{aligned}
& L_y y^k = \lambda T_y y^k + f(t); \\
& h_k \le \max_i \left| g_i \left(y_0^{0,k}, y_{t_1}^{0,k}, \ldots, y_{t_r}^{0,k} \right) - d_i \right|, (i = 0,1,2,\ldots,n); \\
& R\left(h_k, y^k\right) = \left(\frac{g\left(y_0^{1,k}, y_{t_1}^{1,k}, \ldots, y_{t_r}^{1,k}\right) - g\left(y_0^{0,k}, y_{t_1}^{0,k}, \ldots, y_{t_r}^{0,k}\right)}{h_k}, \ldots, \right. \\
& \quad \left. \ldots \frac{g\left(y_0^{n,k}, y_{t_1}^{n,k}, \ldots, y_{t_r}^{n,k}\right) - g\left(y_0^{0,k}, y_{t_1}^{0,k}, \ldots, y_{t_r}^{0,k}\right)}{h_k} \right); \\
& R z^k = g\left(y_0^{0,k}, y_{t_1}^{0,k}, \ldots, y_{t_r}^{0,k}\right) - d; \\
& y_0^{k+1} = y_0^k - z^k, \ \ k = 0,1,2,\ldots .
\end{aligned}\right\} \qquad (6)$$

Для вычисления якобиана, на каждом шаге необходимо решать $n+1$ задачу Коши. В работе [2] для этого использовались аналоговые вычислительные системы. Ниже предлагается использовать квадратурно-разностные методы решения интегро-дифференциальных уравнений, основанные на сочетании разностных методов известных из теории дифференциальных уравнений и квадратурных методов аппроксимации интегрального оператора используемых при численном решении интегральных уравнений. Рассмотрим эти методы применительно к уравнению (4), записав его в виде

$$\begin{gathered}
y^{(n)}(t) = F(t, y(t), y'(t), \ldots, y^{(n-1)}(t)) + \int_0^x K(t, s, y(t), y'(t), \ldots, y^{(n-1)}(t))\, ds, \\
y^{(i)}(0) = y_{i0}, \quad i = 0, 1, \ldots, n-1.
\end{gathered} \qquad (7)$$

Заменой переменных $y = y_1$, $y' = y_2, \ldots, y^{(n-1)} = y_n$ получаем систему уравнений первого порядка

$$\left\{\begin{aligned}
& \frac{dy_1}{dt} = y_2, \\
& \frac{dy_2}{dt} = y_3, \\
& \ldots\ldots\ldots\ldots \\
& \frac{dy_n}{dt} = F(t, y_1, y_2, \ldots, y_{n-1}) + \int_0^x K(t, s, y_1, y_2, \ldots, y_{n-1})\, ds.
\end{aligned}\right. \qquad (8)$$

Используя метод Рунге-Кутты четвертого порядка в сочетании с методом трапеций либо с обобщенным методом Симпсона, получаем следующий алгоритм решения системы (8)

$$\begin{cases} k_1^{(i)} = h\, f(t_i, Y_i), \\ k_2^{(i)} = h\, f(t_i + \dfrac{h}{2},\ Y_i + \dfrac{k_1^{(i)}}{2}), \\ k_3^{(i)} = h\, f(t_i + \dfrac{h}{2},\ Y_i + \dfrac{k_2^{(i)}}{2}), \\ k_4^{(i)} = h\, f(t_i + h,\ Y_i + k_3^{(i)}). \end{cases} \tag{9}$$

$$Y_{i+1} = Y_i + \Delta Y_i, \quad \Delta Y_i = \tfrac{1}{6}(k_1^{(i)} + 2k_2^{(i)} + 2k_3^{(i)} + k_4^{(i)}) \qquad i = 0,1,2\ldots, \tag{10}$$

где $Y_i = (y_{1i}, y_{2i}, \ldots, y_{ni})$,

$$f(t_i, Y_i) = (y_{2i},\, y_{3i}, \ldots, F(t_i, y_{1i}, y_{2i}, \ldots, y_{ni}) + h\sum_{j=0}^{i} A_j \cdot K(t_i, s_j,\, y_{1j}, y_{2j}, \ldots, y_{nj})),$$

$A_1 = A_i = 1/2, A_2 = A_3 = \cdots = A_{i-1} = 1$ для метода трапеций,

$A_j = \begin{cases} 1/3,\ 4/3, 2/3, \ldots, 4/3, 1/3 & (j = 2m+1,\ m = 1,2,\ldots) \\ 1/3,\ 4/3, 2/3, \ldots, 4/3, 5/6, 1/2 & (j = 2m,\ m = 1,2,\ldots) \end{cases}$ для метода Симпсона.

Недостатком данного метода является необходимость многократного вычисления интеграла на каждом шаге, что существенно замедляет время счета и делает затруднительными вычисления на большем числе узлов.

В этом случае эффективным оказывается использование многошаговых методов. Например, многошаговый алгоритм, основанный на методе Адамса в сочетании с методом трапеций либо с обобщенным методом Симпсона, имеет вид

$$Y_{i+1} = Y_i + \frac{h}{24} \cdot (55 f_i - 59 f_{i-1} + 37 f_{i-2} - 9 f_{i-3}), \tag{11}$$

$$Y_{i+1} = Y_i + \frac{h}{24} \cdot (9 f_{i+1} 19 f_i + 5 f_{i-1} + f_{i-2}), \qquad i = 0,1,2\ldots, \tag{12}$$

где $f_i = f(t_i, Y_i)$.

Данный метод не является самостартующим, т.е. необходимо знание начального отрезка решения (в первых четырех точках) для вычисления которого могут быть использованы описанный выше метод Рунге-Кутты, либо метод Адамса первого порядка.

Алгоритм решения

Таким образом, алгоритм решения нелинейной краевой задачи (1) примет следующий вид.

1. Ввод исходных данных о решаемой задаче, начального приближения $y^0(0)$ и требуемой точности решения δ.
2. Решение задачи (1) в форме Коши, используя методы (9)-(10) либо (11)-(12) и определение g_i.

3. Определение величины h_k из условия (6).

4. Решение n задач Коши для определения $y_{t_s}^{i,k}$, $(i=1,\dots n,\ s=1,\dots r)$, используя методы (9)-(10) либо (11)-(12).

5. Вычисление якобиана R по формуле (6).

6. Вычисление поправки z^k, путем решения системы линейных алгебраических уравнений и определение вектора начальных условий y_0^{k+1}.

7. Если выполняется условие $\left\|z^k\right\| \le \delta$, то итерационный процесс заканчивается, в противном случае повторяются шаги 2 — 7.

Решение тестовой задачи

Проиллюстрируем описанный метод результатами численных экспериментов. При этом, для сравнения, будем решать ту же задачу, что и в работе [2]

$$y'' + 2y' - 0.2y^2 - \int_0^x \cos x\, e^{-s}\,(y' + y)\,ds,$$

с краевыми условиями

$$0.3y(0) + 0.3[y'(0)]^2 + y(1) + y'(1) + y(2) + y'(2) = 0.1674,$$

$$0.1y(0) + 0.2[y'(0)]^2 + y(1) + y'(1) + y(2) + y'(2) = -0.1326.$$

Точное решение $y(x) = e^{-x}\cos x$.

В качестве нулевого приближения возьмем значения $y(0) = 0.6$, $y'(0) = -0.6$, при которых, как показано в [2], итерационный процесс решения на аналого-цифровых вычислительных комплексах расходится.

Результаты численного решения данной задачи, реализующего описанный алгоритм в среде Matlab, приведены в таблице 1. При этом задача Коши решалась методом Рунге-Кутта в сочетании методом трапеций (9)-(10), причем шаг дискретизации составил $h = 0.01$, а заданная погрешность – $\delta = 0.001$.

Таблица 1.

Результаты численного решения задачи

Номер итерации	$y(0)$	$y'(0)$	δ
0	0.6000	-0.6000	–
1	0.6912	-1.6816	1.0816
2	0.9802	-1.1120	0.5696
3	0.9969	-1.0074	0.1047
4	0.9992	-1.0008	0.0066
5	0.9992	-1.0008	2.4×10^{-5}

Относительная погрешность решения составила 0.08%.

Выводы

Таким образом, рассмотренный метод, при удачном выборе начального приближения, обеспечивает высокую точность и быструю сходимость решения и может быть эффективным средством реализации динамических объектов, представленных моделями в виде нелинейных интегро-дифференциальных уравнений с краевыми условиями.

Список литературы

1. Верлань, А. Ф. Математическое моделирование непрерывных динамических систем / А. Ф. Верлань, С. С. Москалюк. — К.: Наукова думка, 1988. — 287 с.
2. Верлань, А. Ф. Решение нелинейных интегро-дифференциальных уравнений на аналого-цифровых вычислительных системах типа АЦВС-32 / А. Ф. Верлань, В. А. Краснокутский // Вопросы радиоэлектроники. - Вып. 2,1984, С. 92 — 99.
3. Современные численные методы решения обыкновенных дифференциальных уравнений / Под ред. Дж. Холла, Дж.Уатта. — М.: Наука, 1979. — 385 с.

РЕАЛІЗАЦІЯ МОДЕЛЕЙ ДИНАМІЧНИХ ОБ'ЄКТІВ, ПРЕДСТАВЛЕНИХ У ВИГЛЯДІ НЕЛІНІЙНИХ ІНТЕГРО-ДИФЕРЕНЦІЙНИХ РІВНЯНЬ З КРАЙОВИМИ УМОВАМИ

Д. Е. Контрерас, С. А. Положаєнко

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

Розглянуто постановку r-точкової крайової задачі при описі динаміки об'єктів у вигляді нелінійних інтегро-диференційних рівнянь. Запропоновано ітераційний підхід щодо розв'язання даної задачі, заснований на методі Ньютона.

Ключові слова: динамічний об'єкт, крайова задача, ітераційний процес, метод Ньютона, крок дискретизації, похибка рішення

IMPLEMENTATION OF DYNAMIC OBJECT MODELS PRESENTED AS NONLINEAR INTEGRO-DIFFERENTIAL EQUATIONS WITH BOUNDARY CONDITIONS

D.E. Contreras, S. A. Polozhaenko

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: polozhaenko@mail.ru

The definition of an r-point boundary-value problem for the description of object dynamics with nonlinear integro-differential equations was discussed. To solve this problem, an iterative approach was proposed based on the Newton method.

Keywords: dynamic object, boundary-value problem, iterative process, Newton method, sampling interval, solution error.

УДК 681.5:519.8

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 3, pp. 256-262

ОБРАБОТКА ИНФОРМАЦИОННЫХ ПОТОКОВ И СОСТАВЛЕНИЕ ДЛЯ НИХ РАСПИСАНИЙ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Е. В. Иванченко, В. А. Хорошко, Ю. Е. Хохлачова

Национальный авиационный университет,
пр. Космонавта Комарова, 1, Киев, 03058, Украина; e-mail: manjelka@yandex.ru

Разработаны математические модели однородных систем обработки информации, которые позволяют анализировать и определять эффективность многомашинных (многопроцессорных) систем с числом вычислителей не больше 16. Рассмотрен алгоритм оперативного создания расписаний для многопроцессорных систем управления, которые используют эвристические средства.

Ключевые слова: математические модели, однородные системы обработки, многопроцессорные системы управления, эвристические средства.

Введение

Современный этап развития средств управления и защиты с использованием вычислительной техники характеризируется тенденцией к применению параллельной обработки информации и многопроцессорных систем, которые обладают повышенным быстродействием. Такое быстродействие было достигнуто за счет параллельной обработки задач. Опыт эксплуатации многомашинных (многопроцессорных) систем обработки информации (МСОИ), защиты показал, что большие возможности этих систем могут быть полностью раскрыты только при использовании эффективных методов и средств организации их работы, т.е. обработки информации и оптимальных расписаний информационных потоков.

Задачи управления можно подразделить [1, 2] на независимые и информационно-связанные. Последние можно представить в виде графа (обычно без циклов), вершины которого соответствуют задачам, а дуги определяют информационные связи, тем самым задавая отношение предшествования на множестве задач.

Существующие методы распределения групп задач можно разделить на два вида: допускающие прерывания и без прерываний. Методы распределения без прерываний могут быть как оптимальными, так и субоптимальными. Для получения оптимального расписания используются различные варианты дискретного программирования. Субоптимальные методы при малых затратах ресурсов и времени дают решения, близкие к оптимальным. При их использовании, как правило, осуществляется частичный перебор возможных решений в соответствие с эвристическими правилами.

С учетом того, что системы обработки, защиты и управления в настоящее время в основном имеют многомашинную (многопроцессорную) структуру, воспользуемся моделью многоканальной системы массового обслуживания. При этом в системах процессоры (машины) отожествляются с каналами обслуживания, а задачи – с заявками. Появление систем, адаптируемых к задачам, т.е. меняющих конфигурацию в зависимости от заявок, обусловило необходимость создания адекватных математических моделей систем с перестраиваемой структурой.

Основная часть

Рассмотрим модель [2] однородной системы при наличии приоритетного потока больших задач. При этом задача считается большой, если её ранг больше $N/2$, где N – число машин (процессоров) в системе. Предположим, что на однородную систему (ОС) из N машин (процессоров) поступает пуассоновский поток больших задач с интенсивностью λ. Вероятность поступления задачи с рангом n есть $\lambda_n(\sum_{n>N/2}\lambda_n = 1, \lambda_n > 0)$. Задачи обслуживаются в порядке поступления, причем закон обслуживания является произвольным и индивидуальным для каждого ранга. Если система находится в состоянии j, а i задач находятся в очереди, то вероятность $G_{ij}(t)$ перехода системы в другое состояние за время t определяется следующим образом:

$$G_{ij}(t) = \sum_{\nu>N/2} \lambda \int_0^t [1 - e^{\alpha(t-t_1)}] e^{-\alpha_{t1}} \frac{(\alpha_{t1})}{j!} dH_\nu(t_1);$$

$$G_{ij}(t) = \sum_{\nu>N/2} \lambda \int_0^t e^{\alpha_{t1}} \frac{(\alpha_{t1})^j}{j!} dH_\nu(t_1);$$

$$G_{ij}(t) = \sum_{\nu>N/2} \lambda \int_0^t e^{-\alpha_{t1}} \frac{(\alpha_{t1})^{j-i+1}}{(j-i+1)!} dH_\nu(t_1),$$

где $H_\nu(t_1), \nu > N/2$ – функция распределения времени решения задач ν-го ранга системой. С помощью производящих функций получены условия, при которых период занятости системы имеет конечную длительность – с учетом того, что под периодом занятости понимаем разность между t_k – моментом времени, когда система переходит из занятого состояния в свободное, и $t_k^{'}$ – наибольшим, не превосходящим его моментом времени перехода из свободного состояния в занятое. Помимо этого, с учетом полученных результатов определяется распределение вероятностей того, что в очереди находится некоторое число задач, ожидающих решения. Эта информация позволяет путем изменения числа машин (микропроцессоров) системы регулировать длину очереди и время обработки в необходимых пределах. Однако при обработке потоков сложных задач ОС можно предположить, что в системе из N машин с заданным объемом памяти время обслуживания программ описывается экспоненциальным законом. Предположим также, что в ОС могут одновременно существовать подсистемы всех рангов – от 1 до R, т.е. $N \geq \frac{R(R+1)}{2}$. Выделим в ОС множество из $N \in E(E = \{0,1,...,N\})$ элементарных машин и реструктуризируем его из подсистемы. Обозначим $l_{k,n}^{(t)}$ число подсистем ранга n, образованных в момент времени t посредством реструктуризации, а $l_{s,n}^{'(t)}$ – число p-программ ранга n, находящихся в очереди длиной S в момент t.

Рассмотрим, как воздействует на систему случайный процесс $\Omega(t) = \{l_{k,n}^{(t)}, l_{s,n}^{'(t)} / k \in E, n \neq \overline{1,k}, S = 0,\infty\}$ при условии, что он марковский.

Пусть $P_k^{l_1,...,l_R}$ – вероятность того, что в момент t $N_l\left(\sum_{n=1}^{R} nl_{N1}n(t)\right)$ машин занято обслуживанием p-программ и в очереди занято $N - N_1\left(\sum_{n=1}^{R} nl_{N-N1}n(t)\right)$ мест, при том, что в системе k ветвей. Требуется вычислить: P_{kN} – вероятность того, что в ОС

находится ровно k ветвей; $N_{cp} = \sum_{k=1}^{N} kP_k + N\sum_{S=1}^{\infty} P_{N+S}$ – среднее число занятых машин, $K_3(N) = N_{cp}/N$ – коэффициент занятости ОС, где $P_K \sum P_K^{l_1,\ldots,l_R} = \sum \lim_{t\to\infty} P^{l_1,\ldots,l_R}$ и суммирование ведется по всем возможным разбиениям на подсистемы в предположении, что выполняется условие нормирования $\sum_{k=0}^{\infty} P_k = 1$.

Пусть $K_{k,R}$ – число способов, с помощью которых можно разбить N машин p-программами, максимальный ранг которых равен R. Тогда, просуммировав $N_{k,R}$ и ряд $P_k^{l_1\ldots,l_r}$, получим искомое значение P_k.

Значение $N_{k,R}$ определяется [2,3] по рекуррентной формуле:

$$N_{k,R} = \sum_{j=1}^{R}\sum_{i=1}^{j} N_{k-j,i}$$

при начальных условиях: $N_{k,1} = 1;\ N_{k,k} = 1;\ N_{k,j} = 0;\ k < j.$

Вероятности $P^{l_1\ldots,l_R}$ того, что в ОС равно k ветвей, при определенном разбиении $l_n, l_n^{'}, n = 1, R$, находятся как решение системы линейных уравнений, составленной с использованием методов теории массового обслуживания. Вероятность занятости машин ОС в момент времени $t + \Delta t$ определяется как сумма вероятностей трех несовместимых событий: в момент t N машин производят операцию разбиения массива данных l на некоторые участки, и при этом за время Δt ни одна подсистема не заканчивает обслуживания вспомогательных программ; в момент t занято $N - N_1$ машин, но за время Δt поступила программа ранга $n, n = \overline{1,R}$; в момент t занято $N - N_1$ машин, но за время Δt закончилось обслуживание p-программ ранга $n, n = \overline{1,R}$.

Переходя к пределу $\Delta t \to 0$, а затем при $\Delta t \to \infty$, получаем систему линейных алгебраических уравнений относительно вероятностей $P_k^{l_1\ldots,l_R}$. Решая эту систему, определяем P_k суммированием $P_k^{l_1\ldots,l_R}$ по различным комбинациям $l_1\ldots,l_R$. С помощью вероятностей $P_k, k = 0,\infty$, определяются вероятность отказа в обслуживании, вероятность того, что все машины свободны, среднее число занятых машин, а также другие характеристики системы. Однако, при анализе систем, в которых исполнение заявок основано на обработке информации от разнотипных источников (например, процессоры, устройства ввода-вывода и т.д.), рассмотренные методы исследования ОС не подходят. Для анализа таких систем предлагается модель многоканальной системы массового обслуживания [2]. Она основана на следующих положениях:

1. Узел обработки информации представляет собой ресурсы различных типов, в системе может быть произвольное, но фиксированное число устройств каждого типа.
2. В любой момент времени обработка осуществляется одним из нескольких устройств и имеет фиксированные требования на ресурсы. Множество состояния обработки задачи определяется классом ее принадлежности и фиксированными требованиями на ресурсы.
3. Заявки поступают на систему из одного или нескольких неограниченных источников; определена средняя интенсивность поступления заявок с различными начальными состояниями обработки.
4. Возможны три формы распределения ресурсов (без разделения или мультиплексирования; с разделением; стандартное мультиплексирование). Способ

распределения ресурсов влияет как на скорость обработки, так и на степень параллельности обработки задач системой.

Пусть J – число типов ресурсов; R_i – количество ресурсов i-го типа в системе, $i=\overline{1,J}$; $\overline{j}$ – число классов заявок; M – число различных векторов требований обработки системой допустимых ресурсов системой. Состояние обработки задачи определяется парой (j,k), что означает: обработка принадлежит классу j и требует множество ресурсов, вырабатываемых $\overline{V_k}$. Для удобства обозначений синтезируем изоморфное отображение множества пар $\{(j,k)\}$ на множество $\{l\}$ простых индексов; $L=J\times K$ – число состояний обработки задач; S_l – состояние l обработки задач, $1\le l\le L$ для завершения обработки ОС проходит через последовательность состояний, а ее завершение эквивалентно переходу в заключительное состояние «О», обозначаемое S_o. Время обслуживания требуемой заявки, перешедшей в состояние S_l – это время, в течение которого заявка использует ресурсы до перехода в очередное состояние. Пусть T_l - среднее время обслуживания, требуемое задачей в состоянии $S_l, l=\overline{1,L}$. Оказавшись в состоянии S_l, заявка остается в нем до истечения времени обслуживания. Следующее состояние определяется дискретным марковским процессом, соответствующим матрице $\overline{P}$; $P=(L+1)\times(L'+1)$ – стохастическая матрица переходных вероятностей. Заявки поступают в систему из одного или нескольких неограниченных источников, интенсивность их поступления в начальном состоянии S_l есть λ_l, общая интенсивность $\lambda=\sum_{l=1}^{L}\lambda_l$. Зная λ, можно определить вероятность нахождения заявки в начальном состоянии S_l: $f_l=f_{l/2}$. Распределение начальных состояний заявок определяется вектором $\overline{F}=[f_1,f_2...,f_L]$. Используя $\overline{F}$ и матрицу $\overline{P}$, можно определить $\overline{G}=[g_1,g_2,...,g_L]$, где g_L - среднее число прерываний обработки в состоянии S_l.

В МСОИ предполагается существование постоянных распределений времени обслуживания и интенсивности поступления для каждого класса заявок. Для этого определяется $P_0(\lambda)$ – вероятность того, что обслуживается комбинация $m, m=\overline{1,M}$. Если параметры $g_l, l=\overline{1,L}$, постоянны, распределение времени обслуживания также постоянно и общая интенсивность входного потока не меняется, то анализируемая система имеет фиксированные характеристики потока заявок. Для данного алгоритма распределений заданий и фиксированных характеристик потока заявок мощность системы определяется как интенсивность входного потока.

Граница мощности $\lambda_{\max}$ для МСОИ рассчитывается как интенсивность входных потоков, при которых гарантируется насыщенное независимое от используемого алгоритма распределение заявок.

Для определения $\lambda_{\max}$ МСОИ предлагается следующий метод. Предположим, что g_l – среднее время пребывания заявок в состоянии V_l; K_l – среднее число обслуживания заявок в состоянии S_l и T_l – среднее число пребывания заявок в состоянии S_l – положительные для каждого состояния обработки заданий $\lambda_{\max}$ константы; $\lambda_{\max}$ является решением задачи линейного программирования

$$\lambda_{\max}=\max_{p(\lambda)}\sum_{m=1}^{P}D_mP_m(\lambda).$$

Здесь $P_m(\lambda) \geq 0; D_m = \left(\sum_{l=1}^{l} V_{m,l} K_{l,m} \right) \Big/ \left(\sum_{l=1}^{l} g_l T_l \right), m = \overline{1, M}; l = \overline{1, L-1}$, где $K_{l,m}$ – число заявок из комбинации m в состоянии S_l; $V_{l,m}$ – средняя скорость обработки задачи из комбинации m в состоянии S_l.

Полученная аналитическая модель позволяет определить эффективность системы обработки информации с фиксированными характеристиками входного потока. Так, как задача линейного программирования содержит L ограничений, то не более L переменных $[P_m(\lambda)]$ должно быть ненулевым. Значение $P_m(\lambda) \geq 0$ определяет временной промежуток, в течение которого система должна обрабатывать комбинацию m, чтобы достичь границы M эффективности. Однозначного решения не гарантируется. Если есть несколько экстремальных точек, то любая выпуклая их комбинация также будет экстремальной.

Зная набор $\{P_m(\lambda)\}$, на котором достигается экстремум, можно определить «нежелательные» комбинации $P_m(\lambda) = 0$ и «желательные». Если стремится к достижению максимальной мощности, то следует отдать предпочтение последним. При этом необходимо учитывать расписание для МСОИ. Алгоритмы составления расписаний в многомашинных (многопроцессорных) системах используют задачи распределения информационно-связанных вершин, представленных в виде графа B без ветвлений и циклов. Этот алгоритм был предложен Ю. С. Шварцем.

Для графа B строится матрица A, которая содержит всю информацию, необходимую для составления расписания: условия очередности и время выполнения операций каждой вершиной (процессором). Определение подмножества распределяемых вершин осуществляется по следующим эвристическим правилам:

Шаг 1. Распределение вершин производится с минимизацией временных характеристик простоев.

Шаг 2. В первую очередь выделяются вершины с большим числом предшествий.

Шаг 3. Среди вершин с одинаковым числом предшествований приоритет имеют операторы с меньшим временем выполнения задачи.

Этот алгоритм гарантирует допустимость решения, удовлетворяющего всем требованиям очередности. После каждого распределения производится переформирование матрицы в соответствии с эвристическими правилами [3]. Алгоритм Шварца используется для однородной двухпроцессорной (двухмашинной) системы в предложении, что каждая вершина может реализоваться на любом процессоре в единицу времени. Распределяемые операторы представляются в виде взвешенного орграфа без контуров, при этом ищутся операторы, не имеющие предшественников, и назначаются на определенные процессоры (машины); матрица распределения графа переформировывается с учетом того, что некоторые вершины уже назначены. Затем в матрице ведется поиск строк с нулевыми элементами и вершин, соответствующих этим строкам, причем назначение на процессоры (машины) эти строки получают сразу же или после простоя процессора (машины), чтобы время занятости процессоров (машин) было почти одинаковым, т.е. операторы пропускаются пакетом.

Более совершенным является алгоритм [4], в котором распределение вершин графа по процессорам (машинам) осуществляется с помощью ярусно-параллельной формы представления графа, т.е. разбиения множества X вершин графа $B: X = X_1 V, X_2 V, ..., X_n V$. Все вершины $x \in X_i$ находятся на расстоянии $i = 1$ от начала B. Применение ярусно-параллельной формы позволило разобрать эффективные методы получения расписаний, достаточно близких к оптимальным. Это достигается за счет того, что вместо критерия $\min\{\max T_j\}$, оптимизирующего характеристики, но

требующего большего времени обработки, определяется $\min \sum_{j=1}^{n} T_j^{\Theta}$, причем Θ выбирается из условия $\Theta > \frac{\lg r}{\left[\lg (\max t_{ij}) - tg\ a\right]}$, где $T_j = \sum_{i=1}^{m} t_{ij} x_{ij}; t_{ij}$ – время решения i-й вершины на j-й машине (процессоре), $i = \overline{1,m}$, $j = \overline{1,n}$; a – одно из ближайших решений и $\max(t_{ij})$ значений матрицы $\| t_{ij} \|$;

$$x_{ij} = \begin{cases} 1, \text{если } i - \text{й алгоритм распределен на } j - \text{ю машину,} \\ 0, \text{если } i - \text{й алгоритм не распределен на } j - \text{ю машину.} \end{cases}$$

При этом необходимо учитывать выполнение следующих условий:

$$\sum_{i=1}^{m} x_{ij} \le k, \sum_{j=1}^{n} x_{ij} = l, k = 1,2,...,m.$$

Развитием ранее рассмотренного алгоритма составления расписаний является алгоритм M независимых работ, выполняемых с помощью N идентичных машин (процессоров). Каждая работа характеризируется временем обработки t_i, штрафом за единицу неиспользованного времени Φ_i и директивным сроком $d_i = t_i$ для всех i. Потому целью алгоритма является минимизация общего штрафа

$$C = \sum_{i=1}^{m} p_i (T_i - t_i),$$

где T_i – действительное время выполнения i-й работы. Предлагаемый алгоритм развивает метод ветвей и границ Элмехреби и Пария, в котором отношения предшествования строятся на основе следующих результатов.

Лемма 1. Для $i < j$, если $t_i \le t_j$ и $P_i \ge P_j$, работа i предшествует работе $j (i < j)$ в оптимальном расписании.

Предполагаем, что работы заранее упорядочены по возрастанию $r_i = t_i / P_i$. Если $r_i = r_j$, то работе с меньшим временем присваивается меньший номер, если $P_i = P_j$ и $t_i = t_j$, то номера присваиваются произвольно.

Лемма 2. Существует оптимальное расписание, где работа 1 называется первой.

Правило развития структуры в предполагаемом алгоритме состоит в том, что назначаемая задача с минимальным номером из множества $A[P(k)]$ поступает на первую освободившуюся машину (процессор), причем конфликты разрешаются назначением задачи на машину с меньшим номером. Здесь под $A[P(k)]$ понимается множество задач, которые можно назначить на позицию $(k+1)$.

Для усиления этого алгоритма предлагается обоснование правил ветвления с помощью следующих положений [5].

Теорема. Если существует работа $j \in A[P(k)]$ такая, что $j < \lambda$ является неподходящим первым получателем информации $P(k)$, где $\lambda : T_\lambda = \min T_{md}; m_d \in D$, то $P(k) = \left\{ g^{(\lambda}, ..., g^{(k)}, g^{(i)} \right\}$ – работа, назначенная на позицию i.

Следствие. Если существует работа $j \in A[P(k)]$ такая, что $j < m_d$ для всех $m_d < D$, ветви, ведущие от работы $g(k-1)$ в $P(k-1)$, должны быть вычеркнуты. Этот

процесс называется «ловушкой». Включение в предлагаемый алгоритм «ловушки» обеспечивает следующие преимущества: экономия времени при поиске решения; возможность определения неоптимальных ветвей даже при неэффективности нижней оценки; возможность обходить подвести всех уровней основной ветви.

Выводы

Техника определения границы эффективности «желательных» и «нежелательных» комбинаций, информацию о которых полезно использовать при распределении заявок, на практике может применяться только при исследовании систем процессоров (машин) до 16, для которых число возможных комбинаций весьма невелико.

Предложенные алгоритмы позволяют решать как плановые, так и оперативные задачи. Основное достоинство разработанных алгоритмов – минимальные затраты машинного времени при составлении расписаний для многопроцессорных систем управления и их оптимизации для систем защиты управления.

Список литературы

1. Ленков, С. В. Методы и средства защиты информации в 2-х томах. / Ленков С. В., Перегудов Д. А., Хорошко В. А. – К.:Арий, 2008.
2. Евреинов, Э. В. – Однородные вычислительные системы / Евреинов Э. В., Хорошевский В. Г. – Новосибирск: Наука, 1978. – 318 с.
3. Скорик, В. Н. Мультимикропроцессорные системы / Скорик В. Н., Степанов А. Е., Хорошко В. А. – К.: Техника, 1989. – 192 с.
4. Иванченко, И. С. Оценка эффективности распараллеливания программ для информационных ресурсов / Иванченко И. С., Хорошко В. А. // Сучасний захист інформації, Спец. вип, 2013. – С. 73-81.
5. Хорошко, В. А. Методы составления расписаний для многомашинных систем управления / Хорошко В. А., Моржов С. В. // Проблемы управления и информации, № 3, 2000. – С. 126-129.

ОБРОБКА ІНФОРМАЦІЙНИХ ПОТОКІВ І СКЛАДАННЯ ДЛЯ НИХ РОЗКЛАДІВ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Є. В. Іванченко, В. О. Хорошко, Ю. Є. Хохлачова

Національний авіаційний университет,
пр. Космонавта Комарова, 1, Київ, 03058, Україна; e-mail: manjelka@yandex.ru

Розроблені математичні моделі однорідних систем обробки інформації, які дозволяють аналізувати і визначати ефективність багатомашинних (багатопроцесорних) систем з числом обчислювачів не більше 16. Розглянутий алгоритм оперативного створення розкладів для багатопроцесорних систем управління, які використовують евристичні засоби .

Ключові слова: математичні моделі, однорідні системи обробки, багатопроцесорні системи управління, евристичні засоби.

DATAFLOW PROCESSING AND SCHEDULING IN DATA SECURITY SYSTEMS

Ye.V. Ivanchenko, V.O. Khoroshko, Yu.Ye. Hochlacheva

National Aircraft University,
1, Cosmonaut Komarov Ave., Kyiv, 03058, Ukraine; e-mail: manjelka@yandex.ru

Mathematical models of homogeneous data processing systems were developed to analyze and determine the efficiency of multicomputer (multiprocessor) systems incorporating not more than 16 computers. An on-the-fly scheduling algorithm was examined for multiprocessor control systems using heuristic means.

Keywords: mathematical models, homogeneous data processing systems, multiprocessor control systems, heuristic means.

УДК 004.415.056.5(075)

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 3, pp. 263-271

МЕТОДОЛОГІЯ ОБҐРУНТУВАННЯ ОСНОВНИХ ЗАГАЛЬНОСИСТЕМНИХ ВИМОГ ДО ПРОЕКТУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

І.М. Павлов

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

У статті пропонуються методики у складі методології обґрунтування основних загальносистемних вимог до проектування систем захисту інформації на основі методів групового врахування аргументів, аналогій, експертного оцінювання та статистичного оброблення даних.

Ключові слова: вимоги, властивості, методологія, методики, система захисту інформації.

Постановка проблеми

Визначити напрями розвитку систем захисту інформації можливо лише після обґрунтування основних загальносистемних вимог на основі сучасної методичної бази [1-5]. Аналіз сучасного стану методичного апарату обґрунтування вимог до систем захисту інформації свідчить, що його основним недоліком є використання виключно внутрішніх властивостей системи захисту інформації, без врахування їх «внеску» до систем вищого рівня – інформаційних систем (ІС), а також ототожнення методик оцінювання систем захисту інформації з методиками обґрунтування вимог до них. Крім того, на об'єктах критичної інфраструктури (ОКІ) робота ІС тісно пов'язана зі специфікою цих об'єктів, що накладає особливості на вимоги до систем захисту інформації, як систем критичного застосування цих об'єктів.

У зв'язку з цим, розроблення підходу, який надав би змогу уникнути зазначених недоліків та обґрунтувати основні загальносистемні вимоги до систем захисту інформації, є актуальним науковим завданням.

Аналіз останніх досліджень і публікацій

Аналіз останніх публікацій дає змогу дійти висновку, що сучасні методичні підходи розрізнені й специфічні щодо способу обґрунтування загальносистемних вимог до систем захисту інформації (СЗІ) та мають ряд принципових недоліків. Так, використання методичного підходу [3] дає змогу обґрунтувати лише наближені значення основних вимог до СЗІ, оскільки в ньому для визначення ефективності захисту використовується ряд величин, що важко піддаються формалізації. До таких величин належать гравітаційна модель, яка використовує одиницю ефективності засобів захисту з системи обмежень задач. Методики [4,5] за своєю суттю є оцінювальними, оскільки вхідними даними в них є часткові показники внутрішніх властивостей СЗІ, а не показники систем більш високого порядку (відповідно до ІС у

цілому). В результаті використання таких методик можна дійти висновку лише про відповідність СЗІ «директивно встановленим» вимогам.

Таким чином, *метою* статті є обґрунтування основних загальносистемних вимог до проектування систем захисту інформації на ОКІ.

Основна частина

На початку XXI століття не лише багато зарубіжних країн, а й терористичні і кримінальні структури інтенсивно вдосконалюють методи та способи використання інформаційних технологій і засобів деструктивних впливів на інформаційні ресурси державних, комерційних підприємств та організацій. Таке застосування інформаційних технологій і засобів надає таким застосуванням властивості інформаційної зброї, яка може бути застосована в будь-який час.

З огляду на такі тенденції в більшості країн світу з метою систематизації об'єктів, втрата або порушення нормального функціонування яких призведе до значних або непоправних негативних наслідків для національної безпеки, введено поняття «критична інфраструктура», основою яких є системи критичного застосування [6].

Особливістю систем критичного застосування є те, що інформаційна безпека традиційно зосереджена на досягненні наступних цілей: конфіденційності, цілісності, доступності. Стратегія безпеки традиційної інформаційної технології спрямована, в першу чергу, на конфіденційність із необхідними засобами управління доступом для досягнення заданої мети. Безпека в цих системах стосується підтримки доступності всіх компонентів системи. При цьому, цілісність є часто другою за важливістю задачею.

Задачі забезпечення основних функцій ІС критичного застосування іноді входять всупереч із задачами їх інформаційної безпеки. Це викликано тим, що критичні інфраструктури мають особливості, які суттєво впливають на зміст вимог щодо забезпечення захисту інформації, а саме [7]: наряду з широким застосуванням систем, які мають операційні системи, працюючі в режимі реального часу, ускладненого взаємозв'язку інформаційного захисту з фізичними процесами і наслідками в промисловому секторі – основними видами інформації, що захищається в ІС критичного застосування, є технологічна (забезпечує управління технологіями або чутливо важливими процесами), програмно-технічна (програми системного і прикладного характеру, що забезпечують функціонування об'єктів), командна (управлінська) і вимірювальна, які не належать до інформації з обмеженим доступом (якщо в таких системах циркулює інформація з обмеженим доступом, то вона підлягає захисту згідно з чинними вимогами і нормами технічного захисту інформації).

Враховуючи зазначене, для вирішення питань розглянемо процес захисту інформації, з одного боку, як об'єкт, що містить інші підсистеми, а з іншого – як елемент ІС більш високого порядку.

Загальна структура запропонованої методики (рис. 1) складається з чотирьох основних блоків: блок 1 – формування вихідних даних; блок 2 – визначення системи показників; блок 3 – формування обмежень; блок 4 – розрахунок значень показників основних загальносистемних вимог до СЗІ; блок 5 – визначення рекомендацій.

Вихідними даними для методології визначення основних вимог до СЗІ на ОКІ є (блок 1): показник ефективності захисту інформації в системі критичного застосування, який задається; варіанти типових СЗІ критичного застосування за результатами досліджень; зовнішні та внутрішні фактори впливу на захист інформації в системах критичного застосування; параметри ІС ОКІ. Під показниками СЗІ (блок 2) визначаються властивості СЗІ та задачі, які необхідно розглядати СЗІ.

У таблиці 1 наведені властивості СЗІ як складних ІС (додатково розширений перелік з [8]). Зрозуміло, що цей перелік не є вичерпаним і повинен бути розширеним. Однак вже з його аналізу видно, що умовно властивості СЗІ можна поділити на

незалежні та взаємопов'язані. Тому доцільно побудувати ієрархію необхідних властивостей та визначити відносну важливість кожної властивості. Найменш важливі властивості можуть бути виключені з подальшого розгляду.

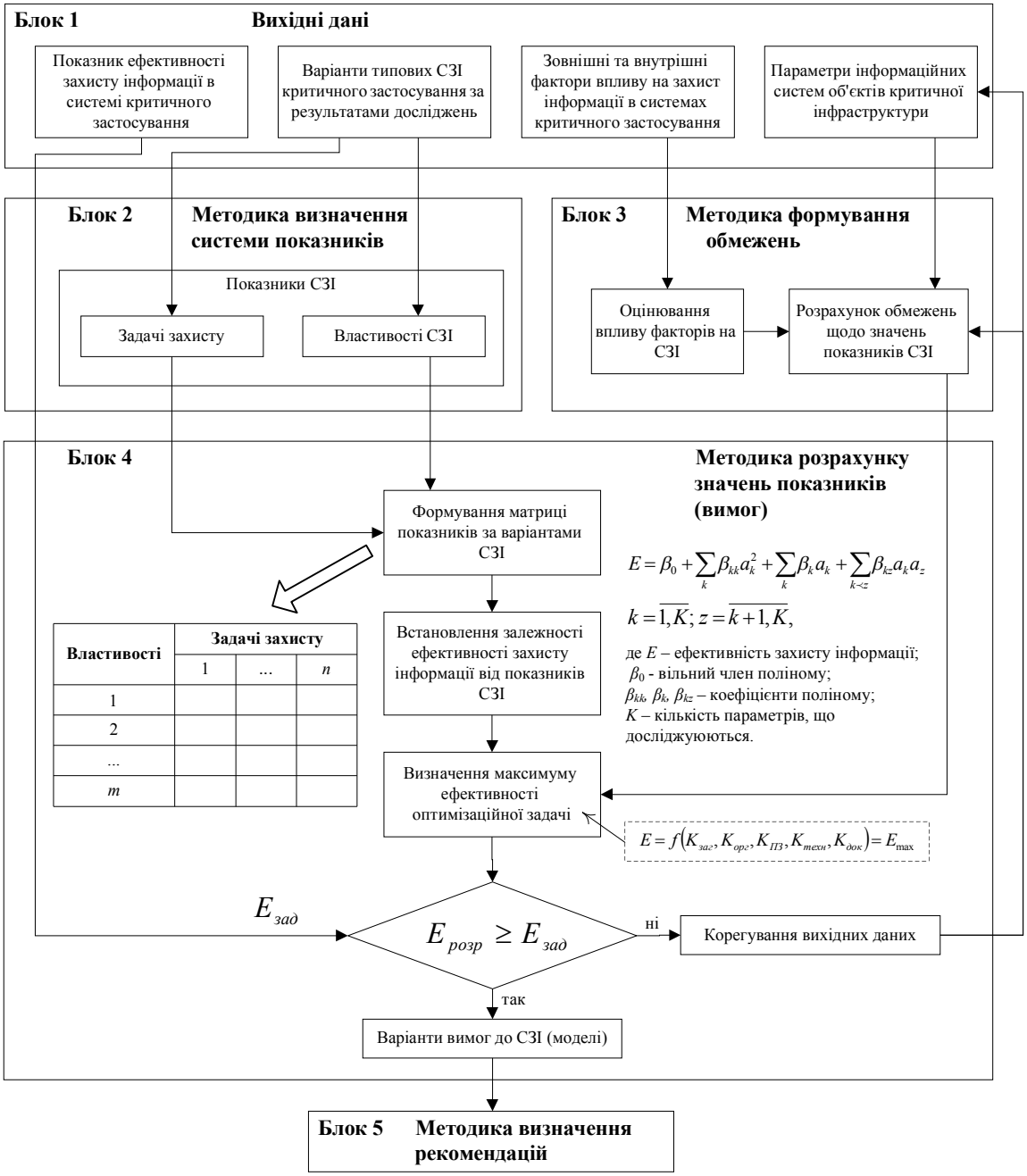


Рис. 1. Загальна структура методології обґрунтування основних загальносистемних вимог до проектування систем захисту інформації ОКІ

У подальшому для кожної властивості (з тих, які залишились) необхідно визначити сукупність показників, які її характеризують, їх відносну важливість стосовно той або іншої властивості, можливий діапазон їх зміни, а також градації значень показників, які відповідають обраній шкалі якості (наприклад, трирівнева шкала: висока, середня, низька). Після цього доцільно визначити важливість кожного показника відносно усієї сукупності показників та найменш важливі з них виключити з подальшого розгляду.

Таблиця 1.

Властивості систем захисту інформації як складних інформаційних систем

Автономність роботи	Адекватність	Безпечність
Здатність до взаємодії	Взаємозамінність	Відновлюваність
Відповідність	Відстежуваність	Придатність до встановлення або монтажу
Гнучкість	Готовність до негайного використання	Деградованість
Довговічність	Доступність за можливістю використання	Доступність за ціною
Експлуатаційна придатність	Ергономічність	Ефективність щодо виконання процесу
Ефективність щодо планування	Живучість	Спроможність виконання критеріїв захисту інформації (конфіденційність, цілісність, доступність, спостережність)
Змінюваність	Інтегрованість	Конструктивність
Придатність до зміни конфігурації	Легальність	Масштабованість
Мобільність	Придатність до модернізації	Придатність до модифікації
Модульність	Надійність	Налаштованість
Аудит	Повторюваність	Працездатність
Пристосованість	Прогнозованість	Простота побудови та використання
Ремонтопридатність	Придатність до негайного розгортання	Розширюваність
Стабільність	Стандартизованість	Стійкість
Сумісність	Тестованість	Точність
Транспортабельність	Універсальність	Чутливість

Окрім того, усі показники доцільно поділити на 2 групи: які не є джерелом протиріч між властивостями, та показники, кращі значення яких для одних властивостей мають наслідком погіршення деяких інших властивостей. Для показників першої групи можна одразу висунути вимогу щодо належності їх значень до діапазону, який відповідає високій якості відповідних властивостей. Показники другої групи вимагають більш детального аналізу та прийняття компромісних рішень щодо їх значень для забезпечення прийнятої якості властивостей, на які вони впливають.

Необхідно зазначити, що формально можуть існувати деякі специфічні показники, що характеризують систему, але які складно віднести до деякої властивості. До таких показників діапазон зміни їх значень доцільно поділити на інтервали, які відповідають обраній шкалі якості самої ІС та висунути вимогу щодо належності їх значень, які реалізуються, діапазону, який відповідає високій якості системи.

Для розрахунку значень та формування матриці показників за варіантами вимог до системи захисту об'єкта $w_i \in W$, $i = \overline{1,n}$, і до процедур над нею, сформулюємо задачі, які припускають оптимізацію по всіх елементах [9]: $M_\tau(w_i) \subseteq M(w_i), \tau = \overline{1,\sigma}$.

Задача 1. Мінімізація вартості забезпечення захисту об'єкта $w_i \in W$, $i = \overline{1,n}$, тобто $S(w_i) = \sum_{j=1}^{k} S_j(w_i)\chi^j(w_i) \to \min_{M_\tau(w_i)}, \tau = \overline{1,\sigma}$ при наступних обмеженнях: $\sum_{j=1}^{k} \chi_\tau^j(w_i) \le k$, $\sum_{j\in J} I_j(w_i)\chi_\tau^j(w_i) \ge J_0(w_i)$, $\sum_{j=1}^{k} S_j(w_i)\chi_\tau^j(w_i) \le S_0(w_i)$, $\chi_\tau^j(w_i) = 1 \vee 0$.

Більш точно задача формується з урахуванням нерівності, яку можна розрахувати з умовою: вартість захисту об'єкта повинна бути мінімізована, принаймні, вона не повинна перевищувати певної величини, скажемо $S(w_i)$:

$$S(w_i) = \sum_{j=1}^{k} S_j^n(w_i)\chi^j(w_i) + \max_{i\in 1} T_0(w_i)\sum_{j=1}^{k} S_j^\ni(w_i)\chi^j(w_i) = S^n(w_i) + \max_{i\in 1} T_0(w_i)S^\ni(w_i) \le S_0(w_i),$$

$w_i \in W$, $i = \overline{1,n}$, тобто з роздільним обліком вартості проектування і експлуатації засобів і методів, застосованих для захисту об'єкта.

Задача 2. Мінімізація ефективності систем захисту об'єкта $w_i \in W : v(w_i) - S(w_i) \to \max_{M_\tau(w_i)}$, при обмеженнях задачі 1.

Задача 3. Мінімізація ймовірності злому всіх методів, які використовуються для захисту об'єкта, при обмеженнях, прийнятих при розв'язку задач 1 і 2: $P(w_i) = 1 - \prod_{j=1}^{k}\left(1 - p_j(w_i)\right)\chi^j \to \min_{M_\tau(w_i)}$.

Задача 4. Максимізація вартості злому усіх методів, які використовуються для захисту об'єкта $w_i \in W$: $C(w_i) = \sum_{j=1}^{k} c_j(w_i)p_j(w_i)\chi^j(w_i) \to \max_{M_\tau(w_i)}$, при обмеженнях задачі 1, а також наступних: $\sum_{j=1}^{k} t_j p_j(w_i)\chi^j(w_i) \ge T_0(w_i)$, $\sum_{j=1}^{k} c_j(w_i)p_j(w_i)\chi^j(w_i) \succ v(w_i)$.

Задача 5. Мінімізація величини втрат від злому всіх методів, які використовуються для захисту об'єкта $w_i \in W$: $\pi(w_i) = \sum_{j=1}^{k} \pi_j(w_i)p_j(w_i)\chi^j(w_i) \to \min_{M_\tau(w_i)}$, при обмеженнях, прийнятих у задачі 4, а також обмеження на вартість злому системи захисту об'єкта: $\sum_{j=1}^{k} \pi_j(w_i)p_j(w_i)\chi^j(w_i) \prec c_0(w_i)$.

Розв'язок зазначених задач дозволить сформувати кращу матрицю за варіантами СЗІ, а розв'язок відповідної сукупності задач для всієї множини об'єктів W - створити сукупність загальносистемних підходів до побудови варіанту СЗІ для системи в цілому.

Основне призначення блока 3 – це формування обмежень на основі врахування зовнішніх і внутрішніх факторів впливу на інформацію та СЗІ. Схематично методика формування обмежень для визначення вимог до СЗІ ОКІ наведена на рис. 2.

Причиною уразливості ОКІ можуть бути недоліки або слабкі місця ІС, захисту інформації, процедур внутрішнього контролю, які можуть бути використані з метою порушення процедур безпеки інформації. Основні зовнішні і внутрішні фактори, які впливають на захист інформації в ОКІ, представлені на рис. 3.

Сукупність вимог до СЗІ докладно представлено в [10]. У загальному випадку доцільно виділити наступні групи вимог до СЗІ: загальні, організаційні, конкретні вимоги до підсистем захисту, технічного і програмного забезпечення, документування, способів і методів захисту. У подальшому проводиться розрахунок обмежень щодо показників СЗІ. Загальний підхід до методики розрахунку значень показників (вимог) (блок 4) наданий на рис. 1.

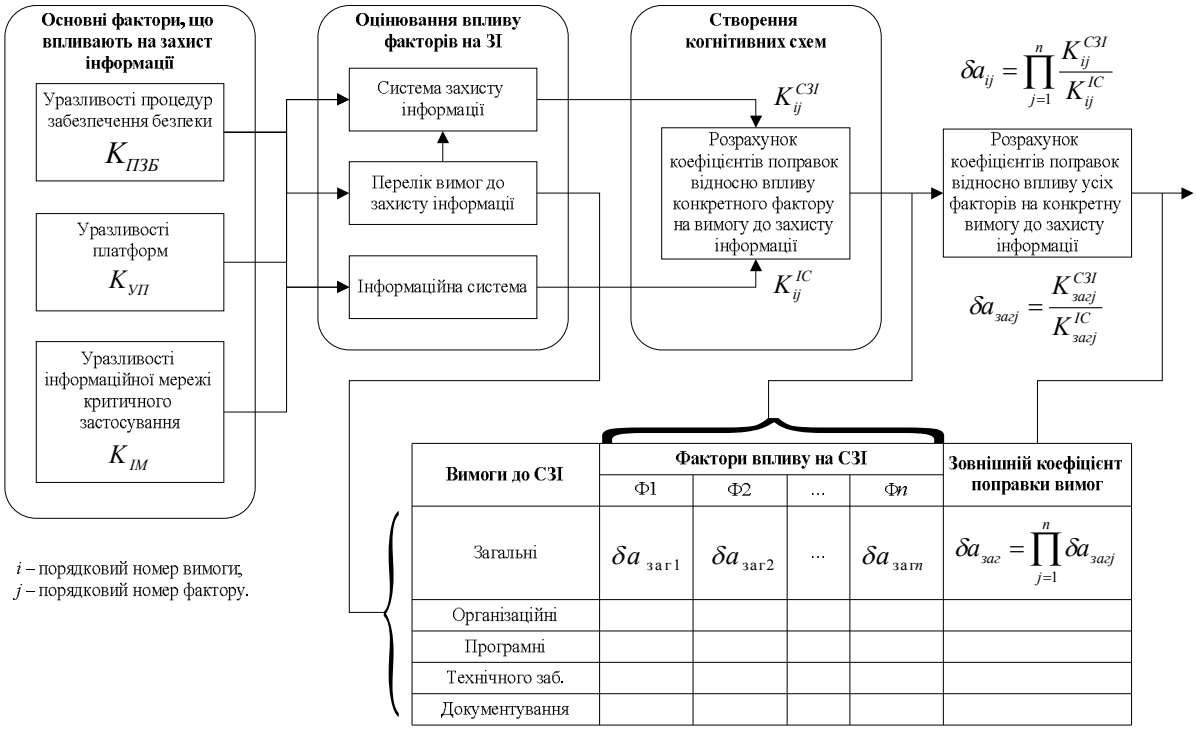


Рис. 2. Методика формування обмежень для визначення вимог до систем захисту інформації ОКІ

Для визначення кінцевого варіанту загальносистемних вимог до СЗІ, які отримані під час розрахунків у блоці 4, необхідно оцінити обґрунтованість рекомендацій, які необхідно прийняти для визначення структури СЗІ на основі багатокритеріального порівняння альтернативних варіантів СЗІ (блок 5), для чого пропонується методика обґрунтування рекомендацій. Як показник обґрунтованості пропонується використовувати ймовірність p_0 того, що альтернативні варіанти СЗІ дійсно є кращими. Відповідно, критерій обґрунтованості має вигляд $p_0 \geq p_z$, де p_z – мінімально припустиме значення ймовірності того, що рекомендовані вимоги до СЗІ дійсно є кращими. Показник p_0 визначається через ймовірність трьох незалежних подій: модель функціонування СЗІ, з використанням якої формується множина альтернативних варіантів, є адекватною; найкращий варіант системи потрапив до переліку порівнювальних альтернатив; з переліку альтернатив методами багато вимірювального порівняльного аналізу були відібрані дійсно найкращі варіанти СЗІ. Тоді критерій обґрунтованості набуває вигляду $p_0 = p_1 p_2 p_3 \geq p_z$, де p_1, p_2, p_3 – ймовірності першої, другої та третьої події відповідно.

Значення показників p_1, p_2, p_3 можна обчислити. Якщо модель функціонування СЗІ отримана на основі методів планування експерименту [11], то ймовірність першої події дорівнює довірчій ймовірності, для значення якої була оцінена адекватність регресійної моделі (зазвичай, 0.9-0.95), тобто p_1=0.90-0.95.

Якщо безпосередньо оцінити адекватність моделі неможливо, тоді доцільно скористатися експертним оцінюванням величини p_1 відповідно до підходу, наведеному в [12], тобто запропонувати експерту надати вербальну оцінку своєї впевненості в адекватності використаної моделі, а потім перевести отриману вербальну оцінку в числову відповідно до співвідношень, які наведені в таблиці 2.

Уразливості процедур забезпечення безпеки
- невідповідність або відсутність процедур забезпечення безпеки; - відсутність підвищення кваліфікації персоналу; - невідповідність архітектури безпеки; - невідповідність або відсутність керівництва з впровадження обладнання; - відсутність відповідальності за адміністрування безпеки; - відсутність або недоліки аудитів в сфері безпеки; - відсутність конкретного плану аварійного відновлення системи у разі збою або аварії; - відсутність змін конфігурації управління.
Уразливості платформ інформаційних систем критичного застосування
- *конфігурація:* ПЗ не оновлюється; ОС та програми безпеки використовуються без випробувань;параметри використовуються за замовчуванням; не зберігаються критичні конфігурації; зберігання незахищених конфігурації даних (паролів і т.п.); - *обладнання:* невідповідне тестування змін системи безпеки; недостатній рівень фізичного захисту; НСД до обладнання; незахищений відділений доступ; подвійні мережеві карти; відсутність документування активів; радіочастотний і електромагнітний імпульси; відсутність резервного електроживлення; втрата контролю навколишнього середовища; відсутність резервування критично важливих компонентів; - *програмне забезпечення:* переповнення буферу; відмова в обслуговуванні; неправильна обробка невизначених, погано визначених або «неприпустимих» умов; використання незахищених протоколів ПД; передача повідомлень в незахищеному вигляді; запуск надлишкових серверів; недостатня перевірка справжності та контролю доступу; відсутність програм безпеки НСД; відсутність реєстрації інцидентів і т.п.
Уразливості інформаційної мережі критичного застосування
- *Конфігурація мережі:* невідповідність архітектури мережевої безпеки; відсутність контролю потоку даних; неякісно налаштовані параметри безпеки обладнання; відсутність резервування конфігурації мережевого пристрою; передача паролів у незахищеному вигляді; недостатньо часта зміна паролів доступу до мережевих пристроїв; неадекватність контролю доступу до мережевих пристроїв; недостатній рівень фізичного захисту мережевого обладнання; НСД до портів мережевого обладнання; - *Периметр мережі:* не визначений периметр безпеки; відсутній або неправильно налаштований між мережевий екран; мережі управління використовуються для трафіку інших типів; управління мережевими сервісами інформаційної мережі критичного застосування реалізується в мережі ІТ; - *Моніторинг мережі:* неадекватні журнали між мережевого екрану; відсутність регулярного моніторингу безпеки в мережі; - *З'єднання:* не ідентифікуються критичні шляхи контролю та управління; використання стандартних протоколів зв'язку; відсутня або недостатня аутентифікація користувачів, даних або пристроїв; відсутність перевірки цілісності з'єднань; - *Бездротові мережі:* невідповідність аутентифікації між бездротовими клієнтами і точками доступу; невідповідний захист даних між бездротовими клієнтами і точками доступу.

Рис. 3. Основні зовнішні і внутрішні фактори, які впливають на захист інформації в системах критичного застосування

Ймовірність другої події розраховується за формулою $p_2 = N_{розр} / N_{заг}$, де $N_{розр}, N_{заг}$ – кількість розглянутих та загальна кількість можливих варіантів СЗІ. У разі використання методу повного перебору $p_2 = 1$.

Оцінку p_3 розглянемо наступним чином. Нехай за результатами застосування n методів багато вимірювального порівняльного аналізу отримана множина варіантів, причому i-й метод розпізнає найкращий варіант з ймовірністю p_i. За результатами застосування n методів j-й варіант за k методами був визначений як найкращий, а $n-k$ методів його найкращим не визнали. Необхідно оцінити достовірність того, що j-й варіант дійсно є найкращим. Достовірність класифікації j-го варіанту як найкращого оцінюється через перевищення порогу похибки класифікації d:

$$\frac{k\prod_{i=1}^{k} p_i + (n-k)\prod_{i=1}^{n-k}(1-p_i)}{k\prod_{i=1}^{k}(1-p_i) + (n-k)\prod_{i=1}^{n-k} p_i} \succ d. \qquad (1)$$

Таблиця 2.

Оцінювання ймовірності першої події за вербальними оцінками експерта

Вербальна оцінка впевненості експерта в адекватності варіанту СЗІ	Ймовірнісний еквівалент
Дуже незначна	0.01-0.1
Незначна	0.1-0.2
Помірна	0.2-0.4
Середня	0.4-0.6
Суттєва	0.6-0.8
Значна	0.8-0.9
Дуже велика	0.9-0.99

Якщо після оцінювання за (1) множина варіантів не пуста, тоді ймовірність наявності у цій множині найкращих варіантів визначається як:

$$p_m = 1 - \left\{1 - \prod_{j=1}^{m}\left[\frac{k_j}{n}\prod_{i=1}^{k_j} p_i + \frac{n-k_j}{n}\prod_{i=1}^{n-k_j}(1-p_i)\right]\right\}. \qquad (2)$$

При цьому вважається, що результати, отримані за різними методами багато вимірювального порівняльного аналізу, є збіжними.

Якщо ж консультації з експертами не проводилися та їх погляди на зміст поняття «раціональний» (оптимальний) варіант невідомі, значення p_3 може бути оцінено як:

$$p_3 = \frac{N_{важ}^{вик} N_{перетв}^{вик} N_{метод}^{вик}}{N_{важ} N_{перетв} N_{метод}}, \qquad (3)$$

де $N_{важ}^{вик}$, $N_{важ}$ – кількість використаних та можливих варіантів урахування важливості показників відповідно; $N_{перетв}^{вик}$, $N_{перетв}$ – кількість використаних та можливих варіантів переходу від реальних значень показників до розрахункових відповідно; $N_{метод}^{вик}$, $N_{метод}$ – кількість використаних та можливих методів порівняння альтернатив відповідно.

Висновки та напрямки подальших досліджень

Встановлена залежність ефективності захисту інформації СЗІ, які проектуються для ОКІ, що ґрунтуються на комплексному використанні методів групового врахування аргументів, аналогій, експертного оцінювання та статистичного оброблення даних. Зазначена залежність покладена в основу підходу до обґрунтування основних загальносистемних вимог до СЗІ. Застосування такого підходу розширює можливості аналізу в предметній області процесів управління складних систем. Напрямком подальших досліджень слід вважати подальше удосконалення та використання наведеного підходу під час удосконалення методичної бази щодо обґрунтування

проектуємих СЗІ та створення (переробки) відповідних нормативно-правових та керівних документів у сфері технічного захисту інформації.

Список літератури

1. Павлов, І.М. Формалізація проектних показників якості захисту інформації комплексної системи захисту інформації [Текст] / І.М. Павлов, В.О. Бірюков. // Захист інформації. – Київ: 2011. – № 2(51). – С. 15 – 21.
2. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Текст] / НД ТЗІ 3.7 – 003 – 05. – К.: 2005. – 35 с.
3. Малюк, А.А. Информационная безопасность: Концептуальные и методологические основы защиты информации / А.А. Малюк. – М.: Высшая школа, 2004. – 280 с.
4. Широчин, В.П. Вопросы проектирования средств защиты информации в компьютерных системах и сетях / В.П. Широчин, В.Е. Мухин. – К.: 2000. – 111 с.
5. Щеглов, А.Ю. Проблемы и принципы проектирования систем защиты информации от НСД [Текст] / А.Ю. Щеглов. // Сборник "Экономика и производство". – М.: 2001. – № 3. – С. 34 – 46.
6. Проект Закону України "Про внесення змін до деякий законів України щодо забезпечення кібернетичної безпеки України" (зареєстрований № 11125 від 31.01.12).
7. Гончар, С.Ф. Проблеми забезпечення інформаційної безпеки критичної інфраструктури держави: актуальність, особливості, вразливості, загрози, завдання / С.Ф. Гончар, О.В. Коваль. // Збірник наукових праць ЦНДІ ЗСУ. Київ: 2013. – № 4 (66). – С. 280 – 291.
8. Потьомкін, М.М. Загальний підхід до формування вимог до складних систем [Текст] / М.М. Потьомкін, А.А. Седляр // Збірник наукових праць ЦНДІ ЗСУ. Київ: 2013. – № 3 (65). – С. 267 – 281.
9. Кобозева, А.А. Анализ информационной безопасности / А.А. Кобозева, В.А. Хорошко. – К.: изд. ГУИКТ, 2009. – 251 с.
10. Павлов, І.М. Проектування комплексних систем захисту інформації / І.М. Павлов, В.О. Хорошко. – К.: вид. ДУІКТ, 2011. – 245 с.
11. Загорка, О.М. Елементи дослідження складних систем військового призначення [Текст] / О.М. Загорка, С.П. Масов, А.І. Сбітнєв, П.І. Стужук. – К.: НАОУ, 2005. – 100 с.
12. Waldrop, M. Toward a Unified Theory of Cognition [Text] / M. Waldrop. – Science. – 1988. – Vol. 241. – № 27. – P. 27 – 29.

МЕТОДОЛОГИЯ ОБОСНОВАНИЯ ОСНОВНЫХ ОБЩЕСИСТЕМНЫХ ТРЕБОВАНИЙ К ПРОЕКТИРОВАНИЮ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЬЕКТАХ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

И.Н. Павлов

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

В статье предлагаются методики в составе методологии обоснования основных общесистемных требований к проектированию систем защиты информации на основе методов группового учёта аргументов, аналогий, экспертной оценки и статистической обработки данных.

Ключевые слова: методология, методики, свойства, система защиты информации, требования.

STRATEGY FOR JUSTIFICATION OF BASIC GENERAL SYSTEM REQUIREMENTS FOR DESIGNING DATA SECURITY SYSTEMS FOR CRITICAL INFRASTRUCTURES

I.N. Pavlov

State University of Telecommunications,
7, Solomenskaya Str., Kyiv, 03680, Ukraine; e-mail: pavlov@ukr.net

In this paper, the authors propose the techniques incorporated into a strategy for justification of basic general system requirements for designing data security systems based on group argument accounting methods, analogy approach, expert assessment methods, and statistical data processing methods.

Keywords: strategy, techniques, features, data security systems, requirements.

УДК 615.252

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 3, pp. 272-277

МАТЕМАТИЧНА МОДЕЛЬ ДИНАМІКИ ГЛЮКОЗИ В ПРОЦЕСІ ЗАСВОЄННЯ ЇЖІ

Ю.М. Чайківська[1], **Р.М. Пасічник**[2]

[1] Тернопільський національний педагогічний університет ім. В. Гнатюка,
вул. Винниченка, 10, м. Тернопіль, 46000, Україна, e-mail: u_chaika@yahoo.com
[2] Тернопільський національний економічний університет,
вул. Львівська, 11, м. Тернопіль, 46000, Україна

В даній статті розглядається динаміка глюкози в крові у процесі засвоєння їжі. Розроблено математичну модель розподілу поступлення глюкози, що використовує найпростішу параболічну залежність. Розроблено математичну модель з використанням експоненціальної функції, що характеризує бурхливіший процес засвоєння глюкози. Було виявлено, що модель з експоненціальною функцією є точнішою.

Ключові слова: неавтономна модель, динаміка глюкози, цукровий діабет, ідентифікація, модель розподілу.

Постановка проблеми

На сьогоднішній день виникає проблема контролю вмісту глюкози в крові у хворих на цукровий діабет. У людському організмі за стабілізацію рівня глюкози в крові відповідає підшлункова залоза, яка виробляє гормони інсулін та глюкагон, що дозволяють збільшити або зменшити концентрацію глюкози. Проте, у хворих на цукровий діабет спостерігається порушення функцій підшлункової залози в поєднанні із заниженою чутливістю до інсуліну. Це призводить до коливання глюкози в крові, як до появи глікемії: гіперглікемії (високої концентрації глюкози), так і гіпоглікемії (низької концентрації). Одним із важливих факторів, що впливають на рівень глюкози є прийом їжі. Варто зазначити, що необхідно спостерігати надходження глюкози з їжею протягом активної доби хворого.

Контроль вмісту глюкози в крові є важливим при аналізі стану хворих на цукровий діабет. Зокрема, цей показник також використовується для вибору режиму харчування хворого. Емпіричний підбір такого режиму містить ризики перевищення граничних максимальних або мінімальних рівнів концентрації глюкози. Ці ризики можна значно зменшити із використанням математичної моделі рівня глюкози в крові.

Тому розробка математичної моделі динаміки глюкози в процесі засвоєння їжі складає актуальну проблему.

Аналіз останніх досліджень і публікацій

Більшість плазмових моделей динаміки глюкози в крові будуються на основі даних внутрівенного тесту толерантності до глюкози (ВТТГ), зокрема, таким чином побудовані моделі Бергмана, Кобелі, Говорки та ін. [1-3]. Суть даного тесту полягає в тому, що людині натще одноразово внутрівенно вводять глюкозу і через регулярні проміжки часу аналізують її динаміку в крові. Здебільшого тест триває три години і через кожні 10 хвилин здійснюють контроль глюкози. Проба на толерантність до

глюкози у хворого на цукровий діабет покаже підвищений рівень глюкози, а показником нормальної толерантності є повернення до вихідного рівня глюкози в крові протягом вищезазначеного часу. Окрім цукрового діабету, показники толерантності до глюкози можуть бути понижені при порушеннях функцій печінки, а також інфекційних захворювань, ожирінню та дії лікарських препаратів [4]. Такі моделі не можуть описати поведінку глюкози протягом доби, оскільки людина харчується впродовж дня. Однак, пероральний шлях надходження глюкози є складнішою задачею для моделювання її динаміки, оскільки необхідно враховувати часте її надходження та процеси засвоєння.

Варто зазначити, що за основу досліджень науковці беруть модель Бретона [5]. Ця модель дозволяє оцінити динаміку глюкози в крові під дією фізичних навантажень. Вона враховує надходження глюкози ззовні, проте це одноразове її поступлення. Відсутні спостереження впливу режиму харчування на динаміку глюкози.

Останнім часом інтенсивно проводяться дослідження контролю глюкози за допомогою інсулінової помпи [6-8]. Проте, інсулінова помпа має ряд недоліків: часте її використання знижує функцію вироблення гормонів підшлунковою залозою, що призводить до її непрацездатності; при виникненні збоїв у роботі пристрою, хворий може опинитися під загрозою, оскільки не буде введено потрібної дози інсуліну і це може призвести до тяжких ускладнень. Тому, важливими залишаються питання самоконтролю глюкози в крові. Для цього необхідно враховувати чинники, які впливають на динаміку глюкози в крові, зокрема, режим харчування.

Формування цілей

Поступлення глюкози ззовні відіграє важливу роль при здійснення контролю глюкози в крові у хворих на цукровий діабет. Зосередження уваги на кількісній оцінці надходження глюкози з їжею та особливості її засвоєння мають очевидну важливість, оскільки цей процес відбувається кожного дня. За допомогою математичних моделей можна провести чисельний експеримент концентрації глюкози в крові, яка залежить від обсягу та складу харчування протягом активної доби. Ідентифікація дозволить оцінити точність запропонованих моделей.

Основна частина

При кожному прийомі їжі, приймаючи всередину крохмаль або цукор, людина споживає вуглеводи. У процесі травлення вуглеводи розщеплюються на глюкозу та інші компоненти, всмоктуючись через стінки кишечника, надходять у кров. Клітини отримують глюкозу, що поступає в них за допомогою кровообігу, перетворюючи її в енергію. Однак для того щоб проникнути всередину клітини, глюкоза потребує особливого гормону – інсулін. Після прийому їжі рівень глюкози в крові підвищується. За рахунок дії гормону інсуліну глюкоза надходить всередину клітини і перетворюється на енергію. Таким чином, рівень глюкози в крові починає знижуватися. Якщо гормон інсуліну абсолютно виробляється менше, ніж це необхідно, або ж не забезпечує проникнення глюкози всередину клітини, то рівень глюкози в крові стане підвищуватися [9].

Основною метою лікування цукрового діабету є підтримання рівня глюкози в крові як можна більш близьким до нормального. На жаль, людина практично не здатна відчувати перепади рівня глюкози від 4 до 10 ммоль/л [9]. Саме в цьому і полягає підступність цукрового діабету, так як високий рівень глюкози в крові неминуче веде до розвитку ускладнень. Тільки регулярний і частий самоконтроль глюкози в крові дозволить уникнути погіршення стану хворого.

В такому випадку доцільно розробити математичну модель, яка дозволить оцінити загальний обсяг глюкози, який поступає в залежності від обсягу та складу харчування протягом доби.

За основу концентрації взята модель Бретона [5]:

$$\begin{cases} \dot{G}(t) = -p_1\left(dG(t) - X(t)\cdot G(t) - \beta Y(t)G(t) + G_M(t)\right), \\ X(t) = -p_2 X + S_i p_2\left(\gamma(t)G(t) - I_b\right), \\ Y(t) = -\dfrac{1}{\tau_{HR}}Y + \dfrac{1}{\tau_{HR}}dH. \end{cases} \quad (1)$$

В цій моделі перше рівняння описує динаміку глюкози в крові, де $dG(t)$ – різниця рівня в плазмі крові від початкового значення глюкози G_b, p_1 – константа, що дозволяє оцінити поглинання інсуліну, $X(t)$ – віддалений інсулін, $G(t)$ – концентрація глюкози в плазмі, β – зміна, що відображає короткі зміни серцевого ритму внаслідок фізичної активності, $Y(t)$ – показує зміни серцевого ритму, $G_M(t)$ – розподіл харчування протягом доби.

Друге рівняння даної моделі описує зміну інсуліну, де p_2 – константа, що характеризує поведінку інсуліну та його активність, S_i – константа, що описує чутливість до інсуліну, $\gamma(t)$ – інтенсивність виробництва інсуліну, I_b – початковий рівень інсуліну.

Третє рівняння даної моделі відображає диференціальну фільтрацію частоти серцевих скорочень, що імітує збільшення витрат енергії під час фізичних навантажень, де dH – зміна серцевого ритму, τ_{HR} – витрата енергії і реакції частоти серцевих скорочень до збільшення витрати енергії.

З даної моделі виключили внутрішній інсулін $X(t)$, серцеве навантаження $Y(t)$ і додали нову зміну $G_M(t)$ – розподіл харчування протягом доби. Тобто, дозоване фізичне навантаження виключили з даної моделі. Таким чином, математична модель розподілу поступлення глюкози зображена нижче.

$$\begin{gathered} \dot{G}(t) = -p_1(G(t) - G_b) + p_2 G_M(t), \\ G(0) = G_0 \end{gathered} \quad (2)$$

Як відомо, процес травлення їжі завершується протягом часу t_0. До цього часу концентрація глюкози в крові повинна досягнути свого максимуму G_x, а в подальшому знижуватися. Цей феномен моделюємо найпростішою параболічною залежністю

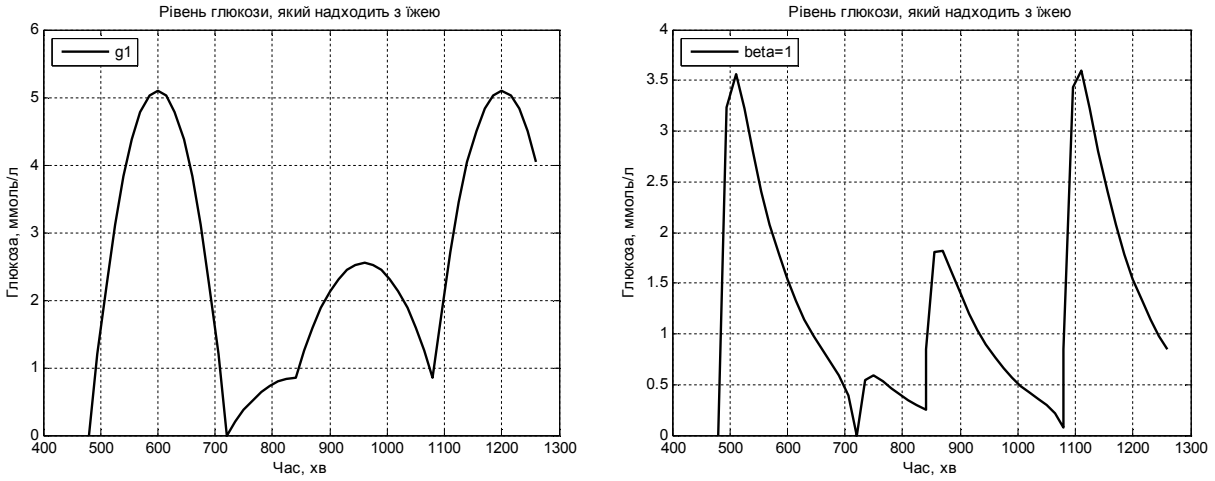
$$G_M(t) = G_x - k(t-120)^{2\alpha}. \quad (3)$$

Глюкоза, яка поступила в кров, засвоюється і розкладається, тому коректність моделі розподілу можна перевірити, співставивши рівень глюкози в крові із рівнем, що прогнозований моделлю, при відповідному представленні $G_M(t)$. Приклад розподілу динаміки глюкози $G_M(t)$, що надходить з їжею, представлено на рис.1а.

Природно припустити, що перша стадія процесу протікає бурхливіше, ніж завершальна. Цей факт моделюємо з використанням експоненціальної функції

$$G_M(t) = G_x - k(t-120)^{2\alpha} \cdot e^{-kt(t-t_0)}. \quad (4)$$

Приклад розподілу динаміки глюкози $G_M(t)$ згідно моделі (4), що надходить з їжею, представлено на рис.1б.



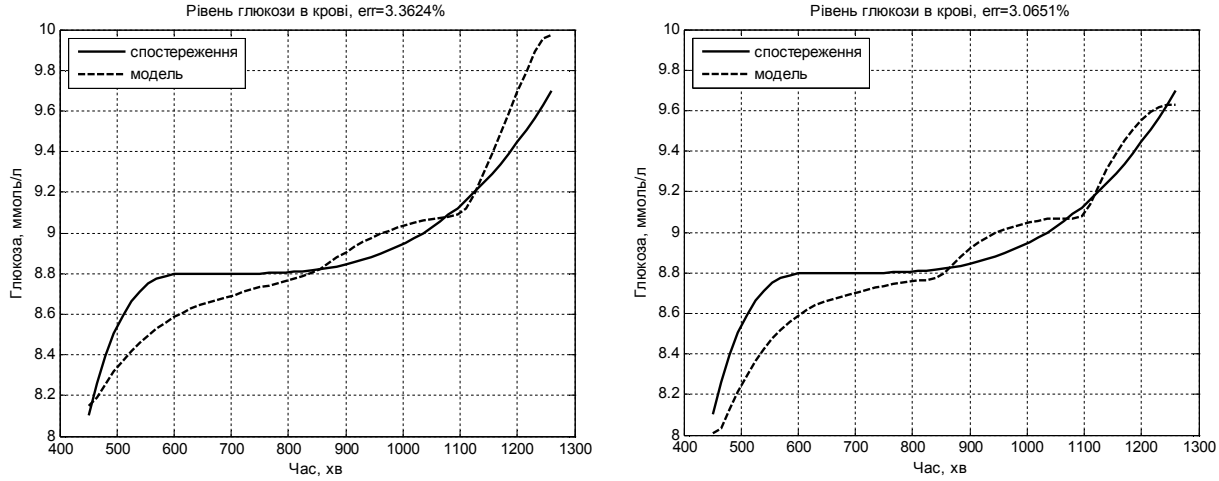
а **б**

Рис.1. Розподіл глюкози $G_M(t)$: а – за моделлю (3); б – за моделлю (4)

На основі даної моделі можна обчислити загальний обсяг глюкози, який поступає в залежності від обсягу та складу харчування. Тому динаміку концентрації глюкози задаємо гіпотетично із перевіркою її адекватності за допомогою моделі (2).

На рис.2а зображено графік спостереження адекватності моделі (3), що відображається параболічною залежністю.

На рис.2б зображено графік спостереження адекватності моделі (3), що використовує експоненціальну функцію.



а **б**

Рис. 2. Спостереження адекватності: а – моделі (3); б – моделі (4)

Похибка прогнозу згідно моделі (3) становить 3.3624%, а для моделі (4) становить 3.0651%.

Таким чином, модель з експоненціальною функцією є точнішою за модель з параболічною функцією. Аналіз чисельних експериментів для інших випадків динаміки глюкози показало аналогічні результати. Оскільки модель (4) дає допустимі похибки, вона може розглядатися як модель динаміки глюкози і спожитої їжі.

Висновки

В даній статті запропоновано моделі динаміки глюкози в процесі споживання їжі. Моделі базуються на даних довготривалих спостережень. Більшість зарубіжних науковців використовують короткотермінові моделі, зокрема, Бергман, Кобелі, Говорка, Д. Рой використовують одноразове введення глюкози і протягом трьох годин спостерігають її динаміку. Проте, важко зробити прогноз рівня глюкози в крові внаслідок таких спостережень, оскільки пероральний шлях надходження глюкози є складнішою задачею для моделювання її динаміки, необхідно враховувати часте її надходження та процеси засвоєння. На основі моделі Бретона запропоновано модель розподілу поступлення глюкози в кров в ході заданого процесу. Модель з експоненціальною функцією є точнішою за модель з параболічною функцією на 0.2973%. Адекватність даної моделі підтверджено експериментальними дослідженнями.

Список літератури

1. Cobelli, C. GIM simulation software of meal glucose–insulin model / C. Cobelli, et al. // Journal of Diabetes Science and Technology. — 2009. —№3 (1). — PP. 44-55.
2. Breton, M. Silico preclinical trials: a proof of concept in closed-loop control of type 1 diabetes / M. Breton, et al. // 2006 IEEE EMBS Conference, New York.—2006. — PP. 5647-5650.
3. Hovorka, R. Evaluation of glucose controllers in virtual environment: methodology and sample application / R. Hovorka, M.E. Wilinska, L.J. Chassin // Artificial Intelligence in Medicine. — 2004. — №32 (3). — PP. 171-181.
4. Bergman, P.J. A Comparison Between the Minimal Model and the Glucose Clamp in the Assessment of Insulin Sensitivity Across the Spectrum of Glucose Tolerance / P.J. Bergman, et al. // Diabetes. — 2004. — №43. — PP. 1114-1121.
5. Breton, M.D. Physical activity--the major unaccounted impediment to closed loop control / M.D. Breton // Diabetes Sci Technol. — 2008. — №2(1). — PP. 169-174.
6. Marchetti, G. , A feedforward-feedback glucose control strategy for type 1 diabetes mellitus / G. Marchetti, et al. // Journal of Process Control. — 2008. — 18(2). — PP. 149-162.
7. Renard, E. Closed-loop insulin delivery using a subcutaneous glucose sensor and intraperitoneal insulin delivery / E. Renard, et al. // Diabetes Care. — 2010. — 33(1). —PP. 121-127.
8. El-Khatib, F.H. Adaptive closed-loop control provides blood-glucose regulation using dual subcutaneous insulin and glucagon infusion in diabetic swine / F.H. El-Khatib, et al. // Journal of Diabetes Science and Technology. — 2007. — №1(2). — PP. 181-192.
9. Швець, О.В. Дієта при цукровому діабеті. / О.В. Швець // Міжнародний ендокринологічний журнал. — 2013. — 2(50). — С. 65-74.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ДИНАМИКИ ГЛЮКОЗЫ В ПРОЦЕССЕ УСВОЕНИЯ ПИЩИ

Ю.М. Чайкивская[1], Р.М. Пасичник[2]

[1]Тернопольский национальный педагогический университет им. В. Гнатюка,
ул. Винниченка, 10, г. Тернополь, 46000, Украина, e-mail: u_chaika@yahoo.com
[2]Тернопольский национальный экономический университет,
Ул. Львовская, 11, г. Тернополь, 46000, Украина

В данной статье рассматривается динамика глюкозы в крови в процессе усвоения пищи. Разработана математическая модель распределения поступления глюкозы использует простейшую параболическую зависимость. Разработана математическая модель с использованием экспоненциальной функции, характеризующая ускоренный процесс усвоения глюкозы. Было обнаружено, что модель с экспоненциальной функцией является точнее.
Ключевые слова: неавтономная модель, динамика глюкозы, сахарный диабет, идентификация, модель распределения

MATHEMATICAL MODEL OF BLOOD GLUCOSE DYNAMICS DURING DIGESTION

Iu.M. Chaikivska[1], R.M. Pasichnyk[2]

[1]Ternopil V. Hnatiuk National Pedagogical University,
10, Vynnychenko Str., Ternopil, Ukraine, 46027; e-mail: u_chaika@yahoo.com
[2]Ternopil National Economic University,
11, Lvivska Str., Ternopil, 46000, Ukraine

In this paper, blood glucose dynamics during digestion is discussed. A mathematical model of glucose uptake distribution was developed based on the simplest parabolic law. Additionally, a mathematical model was developed based on the exponential function to characterize the accelerated process of glucose digestion. It was found that the model based on the exponential function is more accurate than that based on the simplest parabolic law.
Keywords: non-autonomous model, glucose dynamics, diabetes mellitus, identification, distribution model.

UDC 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 3, pp. 278-284

IMPROVEMENT OF THE ACCURACY OF DETECTION OF CLONED REGIONS IN DIGITAL IMAGES

Ye. Yu. Lebedeva

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: whiteswanhl@yahoo.com

In this work, modifications of the method for the detection and location of cloned regions were developed to improve the detection accuracy. Based on the results of experiments and observations performed, we proposed the block types which provide the highest accuracy of detection, with the accuracy assessed by the ratio of area of detected cloned region to actual area of cloned region.

Keywords: accuracy of detection, region area, image falsification, falsification detection, cloning.

Introduction

Digital images (DI) used in the printed media, medicine, science, forensic proceedings, etc., are of primary importance in cyberspace. Currently, various falsifications of digital images performed with graphics editors such as Adobe Photoshop, GIMP, etc., are very common. Digital falsification has become widespread due to the simplicity of use of these graphics editors. Cloning is one of the commonest methods used for falsification of digital images, because it is easily implemented and hardly detected due to the fact that the cloned region is a part of the digital image subjected to falsification. When being embedded into an original image, a cloned region (clone) may have an arbitrary (nonrectangular) shape ensuring its visual inconspicuousness. Therefore, the development of methods for the detection and location of cloned regions to improve the detection accuracy is of current importance.

Statement of the problem and purpose of the study

To create a cloned region with graphics editors such as Adobe Photoshop and GIMP, one can use *Rectangular Marquee Tool*, *Lasso Tool*, *Clone Stamp Tool*, etc. For improved visual embedding of cloned regions, *Eraser Tool* and *Blur Tool* can be used. All the tools mentioned make it possible to create a cloned region of an arbitrary (irregular) shape.

In [1, 2], a method has been developed to detect and locate cloned regions; with the first stage of that method, a digital image is divided into a set of standard-shape overlapping blocks. For the purpose of methodology, a standard block means a square-shape block of any size. The results of experiments have shown that the use of standard blocks does not make it possible to accurately estimate the dimensions and determine the location (shape) of detected falsification regions.

The *Purpose* of the study was to develop modifications of the method for the detection and location of cloned regions in order to improve the detection accuracy.

The detection accuracy was assessed by the percentage ratio of the area of detected cloned region to the actual area of cloned region. The actual area of cloned region was determined as the difference between the original image and the falsified image. The area was measured in pixels.

To accomplish the purpose of the work, the following problems were to be solved:

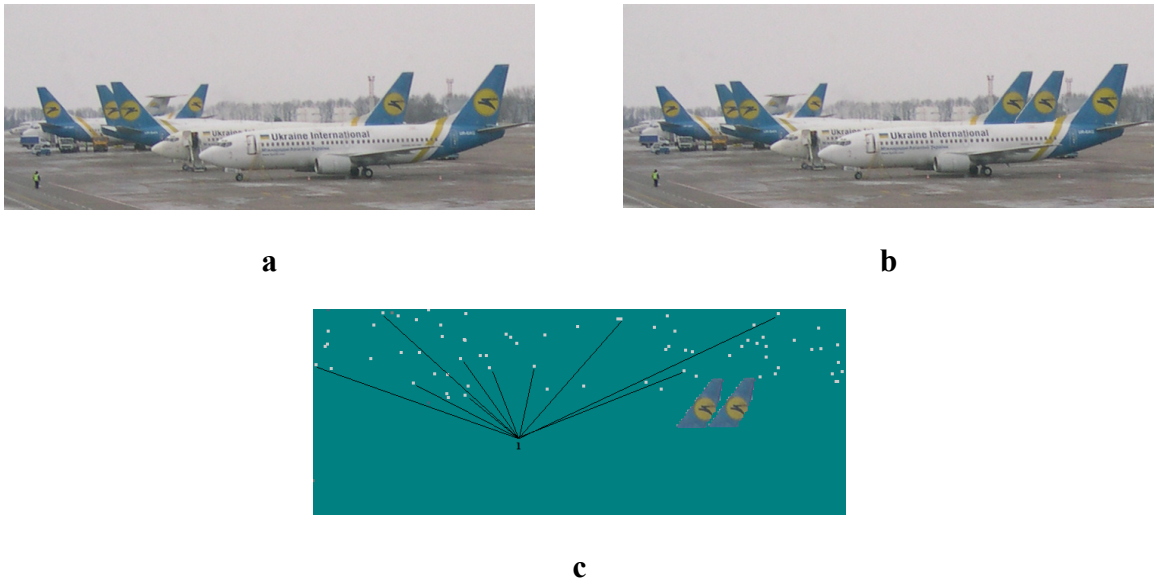
- to find the ways to improve the accuracy of detection of a cloned region,
- to modify the method for the detection and location of cloned regions in order to use the adaptive subdivision of the blocks,
- to modify the method for the detection and location of cloned regions in order to use non-standard blocks within the detection process, and
- to analyze the efficiency of the algorithms developed based on the accuracy of detection of cloned regions.

The ways to improve the accuracy of detection of a cloned region

We assume that there is a digital image $I(m,n)$ with brightness matrix Y. Briefly, the procedure of the method for the detection and location of cloned regions in a DI is as follows [1, 2].

1. Divide the brightness matrix Y of a DI into $p \times p$ overlapping blocks $C = \{c_1, c_2, \ldots, c_s\}$, $\bigcup_{i=1}^{s} c_i = Y$, (here each block c_i is obtained by a single-pixel right shift, left shift, down-shift or up-shift of block c_{i-1}).
2. For each pair of blocks $c_i, c_j, i = 1,\ldots,s, j = i+1,\ldots,s$ calculate the proximity measure $\delta = Metrica(c_i, c_j)$.
3. Analyze the values of proximity measure δ to determine the pairs of blocks c_i, c_j belonging to cloned regions and to a clone prototype.

Square blocks of any size may be used to detect clones with the method proposed (hereinafter referred to as a "basic method"). The results obtained from the computational experiments proved that 8×8 blocks are the most efficient for the detection of cloned regions. Although the use of 4×4 blocks may improve the accuracy of located cloned regions, it may also result in appearance of false-positive blocks (Fig. 1).



a **b**

c

Figure 1. An example of appearance of false-positive blocks: a – original image, b – falsified image, c – result of the use of 4×4 blocks for the detection of cloned regions (here 1 denotes false-positive blocks)

Therefore, the method presented operates with square-shape blocks of size $p \times p$, and this size remains unchanged during the procedure of the method. These features make the basic method non-effective in accuracy of detecting cloned regions.

Hence, the main ways to improve the accuracy of detection of cloned regions are as follows:

1. To use the non-square blocks;
2. To use different block sizes during the detection of cloned regions.

Method for the detection and location of cloned regions using the adaptive subdivision of the blocks

Although in the detection of cloned regions, the use of 4×4 blocks provides for the improvement in detection accuracy, it is reasonable to use this block size not for the entire digital image, but for the potentially falsified regions only.

Let us modify the basic method for the detection and location of cloned regions in a DI in the following way: if detected, the potentially falsified regions are divided into blocks of a smaller size, and the basic method is applied to the blocks newly obtained for the detection of cloned regions.

Briefly, the procedure of the method for the detection and location of cloned regions in a DI using the adaptive subdivision of the blocks is as follows.

1. Divide the brightness matrix Y of a DI into $p \times p$ overlapping blocks $C = \{c_1, c_2, \ldots, c_s\}$, $\bigcup_{i=1}^{s} c_i = Y$, (here each block c_i is obtained by a single-pixel right shift, left shift, down-shift or up-shift of block c_{i-1}).
2. For each pair of blocks $c_i, c_j, i = 1, \ldots, s, j = i+1, \ldots, s$ calculate the proximity measure $\delta = Metrica(c_i, c_j)$.
3. Analyze the value of proximity measure δ to determine the pairs of blocks c_i, c_j suspected for belonging to cloned regions and to a clone prototype.
4. If the potentially falsified blocks are found,
   4.1. divide pairs of blocks c_i, c_j into blocks of a smaller size, $C^i = \{c_1^i, c_2^i, \ldots, c_d^i\}$ and $C^j = \{c_1^j, c_2^j, \ldots, c_d^j\}$, $\bigcup_{n=1}^{d} c_n^i = c_i$, $\bigcup_{m=1}^{d} c_m^j = c_j$,
   4.2. calculate the proximity measure $\delta^{ij} = Metrica(c_n^i, c_m^j)$, and
   4.3. analyze the value of proximity measure δ^{ij} to determine pairs of blocks c_n^i and c_m^j suspected for belonging to cloned regions and to a clone prototype.

Figure 2 shows an example of the results of application of the method for the detection and location of cloned regions in a DI using the adaptive subdivision of the blocks.

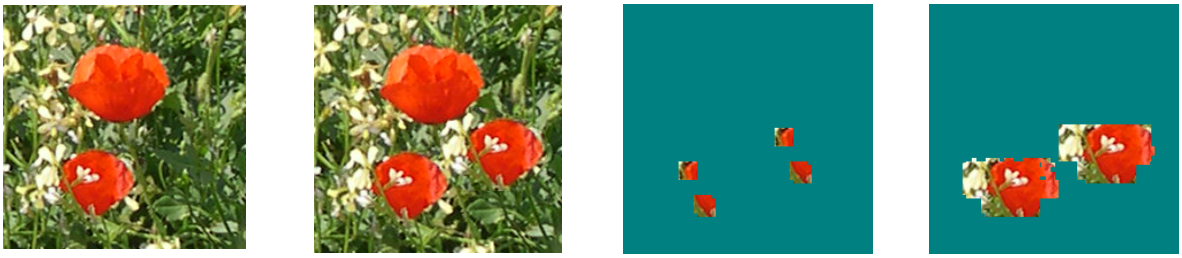
Method for the detection and location of cloned regions using non-standard blocks

Let us consider the use of blocks of non-standard shape (such as triangular blocks and blocks of complex shape) for the detection of cloned blocks.

In [3, 4], the procedure of obtaining triangular-shaped blocks has been discussed in detail. During the experiment, we found the subdivision into triangular blocks that provides higher accuracy of detection with respect to other subdivisions (Fig. 3a).

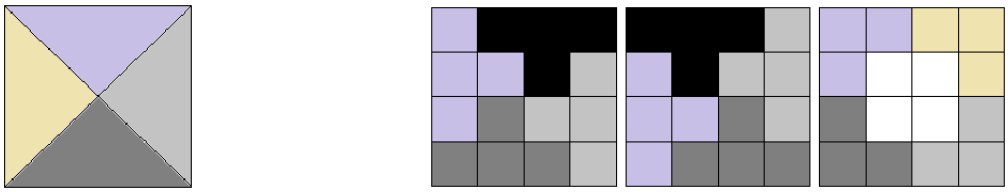
To obtain blocks of complex shape, let us use square blocks (e.g., 16×16 blocks), and divide them into 4×4 blocks. Grouping of 4×4 blocks in a subblock determines the division

of a square-shape block into blocks of complex shape. The computational experiment determined the divisions of blocks of complex shape that provide the highest accuracy of detection with respect to other blocks of complex shape (Fig. 3b).



a **b** **c** **d**

Figure 2. Results of the application of the method for the detection and location of cloned regions using the adaptive subdivision of the blocks: a – original image, b – falsified image, c – use of 16×16 blocks without the adaptive subdivision, d – use of 16×16 blocks with the adaptive subdivision



a **b**

Figure 3. DI matrix blocks that provide the highest accuracy of detection of a cloned region: a – blocks of triangular shape, b – blocks of complex shape.

Let us modify the basic method for the detection and location of cloned regions in a DI in order to use non-standard blocks while detecting the clones.

Briefly, the procedure of the method for the detection and location of cloned regions in a DI using the non-standard blocks is as follows.

1. Divide the brightness matrix Y of a DI into $p\times p$ overlapping blocks $C=\{c_1,c_2,\ldots,c_s\}$, $\bigcup_{i=1}^{s} c_i = Y$, (here each block c_i is obtained by a single-pixel right shift, left shift, down-shift or up-shift of block c_{i-1}).

2. For a block pair considered, $c_i, c_j, i=1,\ldots,s, j=i+1,\ldots,s$, obtain non-standard subdivisions c_i^r and c_j^r, respectively, where r is a subdivision number. For each subdivision:

3. Calculate the proximity measure $\delta = Metrica(c_i^r, c_j^r)$.

4. Analyze the value of proximity measure δ .to determine pairs of blocks c_i^r and c_j^r suspected for belonging to cloned regions and to a clone prototype.

Analysis of the efficiency of the methods developed

A computational experiment was performed to analyze the efficiency of the methods developed based on the accuracy of detection of cloned regions. Within the experiment, the

size of a cloned region was arbitrarily selected depending on the specific image, and irrespective of the size of subdivision blocks used in experiments.

All digital images had the varying depth resolution of the space depicted, and were subjected to falsification and postprocessing by means of Adobe Photoshop and GIMP. Original digital images had various compression ratios corresponding to quality Q setting 4 to 10 in Adobe Photoshop. After application of cloning technology, the falsified digital images obtained were saved using lossless BMP format. The cloned region boundary was subjected to blurring.

The experiment made it possible to obtain the following:

- digital images containing the cloned region detected with the use of non-standard blocks and the adaptive subdivision (Fig. 4),
- ratios of area of detected cloned region to actual area of cloned region for different block types and for the adaptive subdivision (Table 1), and
- detection of cloned regions if they failed to be detected with blocks of square shape (Fig. 5).

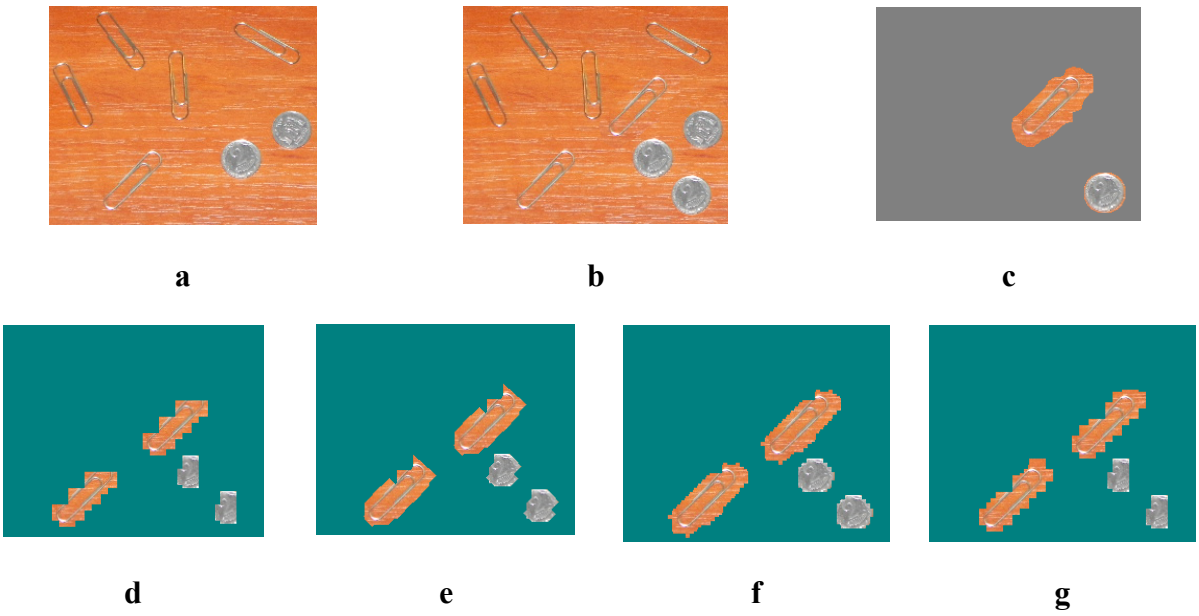


Figure 4. Results of the application of the method of detection of cloned regions using the blocks of non-standard shape and the adaptive subdivision of blocks: a – original image, b – falsified image, c – cloned region, d – use of 16×16 blocks of square shape, e – use of 16×16 blocks of triangular shape, f – use of 16×16 blocks of complex shape, g – use of the adaptive subdivision of 16×16 blocks

Table 1.

Accuracy of the detection of a cloned region with blurred boundaries using the blocks of various types of subdivision and adaptively subdivided blocks

Types of subdivision	Percentage ratios of area of detected cloned region to actual area of cloned region		
	Max.	Min.	Average
Blocks of square shape	56.63	8.58	29.07
Blocks of triangular shape	68.25	23.95	43.51
Blocks of complex shape	73.73	43.28	55.40
Adaptively subdivided blocks	65.00	35.20	53.02

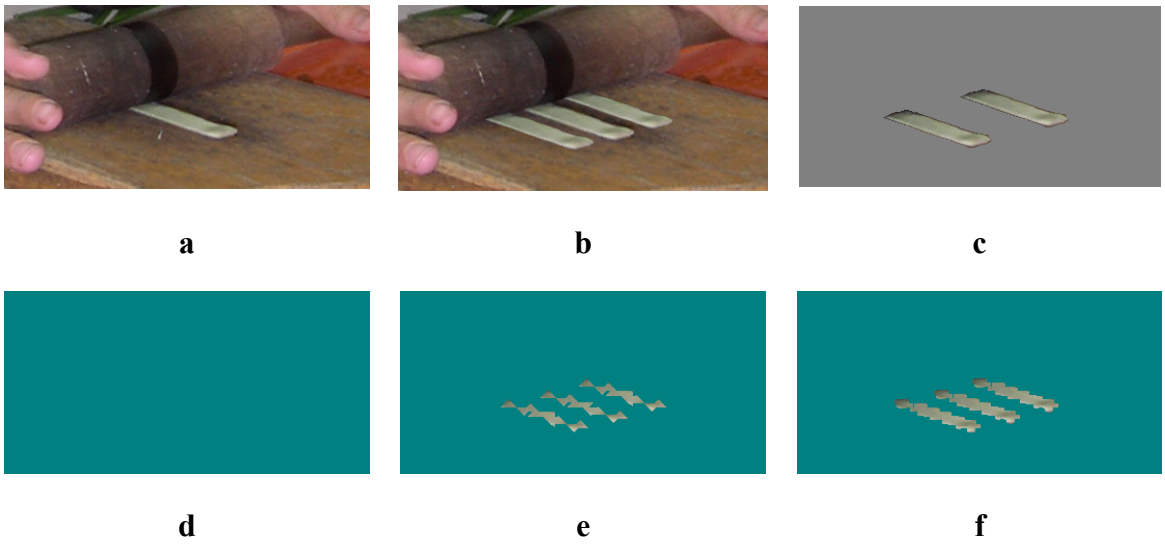


Figure 5. Results of the detection of cloned regions: a – original image, b – falsified image, c – cloned region, d – use of 16×16 blocks of square shape, e – use of 16×16 blocks of triangular shape, f – use of 16×16 blocks of complex shape

The results presented in Table 1 indicate that blocks of complex shape and adaptively subdivided blocks provide higher accuracy than those of square shape and triangular shape. If blocks of triangular shape, complex shape or adaptively subdivided blocks are used in the method for the detection and location of cloned regions, than the percentage ratio of area of detected cloned region to actual area of cloned region increases 1.5 times, 1.91 times and 1.82 times, respectively, compared with the use of standard subdivision.

Conclusions

The ways of modifying the basic method for the detection and location of cloned regions were found to improve the accuracy of detection of a cloned region.

By modifying the basic method, the following two methods were developed: the method for the detection and location of cloned regions using adaptively subdivided blocks, and the method for the detection and location of cloned regions using blocks of non-standard shape.

The efficiency of the algorithms developed was analyzed based on the accuracy of detection of cloned regions. The analysis has shown that the use of blocks of complex shape and adaptively subdivided blocks is more effective.

References

1. Лебедева, Е.Ю. Исследование метрик используемых при обнаружении клонированных участков изображений в задачах выявления фальсификации / Е.Ю. Лебедева, Ю.Ф. Лебедев // Вісник національного технічного університету «ХПІ». – 2011. – №35. – С.25-31.
2. Лебедева Е.Ю. Обнаружение клонированных участков изображений в задачах выявления фальсификации / Е.Ю. Лебедева // XII міжнародна науково–практична конференція «Современные информационные и электронные технологии». – 2011. С. 175.
3. Лебедева, Е.Ю. Использование треугольных блоков для определения области фальсификации в изображениях / Е.Ю. Лебедева, П.Е. Баранов // Інформаційна безпека. – 2011. – №2. – С.27-32.
4. Баранов, П.Е. Виявлення області фальсифікації цифрового зображення блоками трикутної форми / П.Е. Баранов, О.Ю. Лебедева // Інформатика та математичні методи в моделюванні. – 2011. – Том 1, №3. – С. 274-280.

ПІДВИЩЕННЯ ТОЧНОСТІ ВИЗНАЧЕННЯ ОБЛАСТІ КЛОНУВАННЯ В ЦИФРОВИХ ЗОБРАЖЕННЯХ

О.Ю. Лебедєва

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

У роботі розроблені модифікації метода виявлення і локалізації областей клонування для підвищення точності визначення клонованих областей. За результатами експериментів та спостереженнями запропоновані види блоків, що дають найкращу точність визначення, яка оцінюється відносною похибкою величини площі клона до реальної площі області клона.
Ключові слова: точність визначення, площа області, фальсифікація зображення, виявлення фальсифікації, клонування.

ПОВЫШЕНИЕ ТОЧНОСТИ ОБНАРУЖЕНИЯ КЛОНИРОВАННЫХ ОБЛАСТЕЙ В ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ

Е.Ю. Лебедева

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

В работе разработаны модификации метода выявления и локализации областей клонирования для повышения точности обнаружения клонированных областей. По результатам экспериментов и наблюдений предложены виды блоков, дающие наилучшую точность обнаружения, оцениваемую относительной величиной площади выявленной области клона к реальной площади области клона.
Ключевые слова: точность обнаружения, площадь области, фальсификация изображения, выявление фальсификации, клонирование.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 4, номер 3, 2014. Одеса – 95 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 4, номер 3, 2014. Одесса – 95 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 4, No. 3, 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 №1 від 29.08.2014)

Адреса редакції: Одеський національний політехнічний університет,

проспект Шевченка, 1, Одеса, 65044 Україна

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

E-mail: immm.ukraine@gmail.com