Міністерство освіти і науки України
Вінницький національний технічний університет
Національний технічний університет України "КПІ"
Інститут кібернетики НАНУ
Південний Федеральний Університет (Росія)

Тези доповідей першої Міжнародної науково-практичної конференції "Методи та засоби кодування, захисту й ущільнення інформації"

м. Вінниця, Україна
15-17 травня 2007 року

Тезисы докладов первой Международной научно-практической конференции "Методы и средства кодирования, защиты и сжатия информации"

г. Винница, Украина
15 - 17 мая 2007 года

ВНТУ 2007

УДК 681.32+621.391
М54

Відповідальний редактор В.А. Лужецький

Матеріали статей опубліковані в авторській редакції

М54 **Методи та засоби кодування, захисту й ущільнення інформації.** Тези доповідей першої Міжнародної науково-практичної конференції. м. Вінниця, 15-17 травня 2007 року. – Вінниця: ВНТУ, 2007. – 140 с.

Збірка містить матеріали доповідей першої Міжнародної науково-практичної конференції з сучасних проблем кодування, захисту й ущільнення інформації за чотирма основними напрямками: методи та засоби кодування інформації; методи та засоби захисту інформації; методи та засоби ущільнення інформації; методи та засоби перетворення форм інформації

УДК 681.32+621.391

ЗМІСТ

1.Методи та засоби кодування інформації

2. Методи та засоби захисту інформації

3. Методи та засоби ущільнення інформації

4. Методи та засоби перетворення форм інформації

1. Методи та засоби кодування інформації

УДК 621.394.147

МЕТОДИ ЦИФРОВОЇ МОДУЛЯЦІЇ ПОСЛІДОВНОСТЯМИ ГАЛУА

Л.Б. Петришин (L. Petryshyn), д.т.н., професор
Гірничо-металургійна академія, м. Краків, Польща
(AGH University of Science and Technology Krakow, Poland)
e-mail: petryshynl@poczta.fm, petryshynl@mail.ru

В. Кубіньский (W. Kubiński), д.т.н., професор
Гірничо-металургійна академія, м. Краків, Польща
(AGH University of Science and Technology Krakow, Poland)
e-mail: wkubinsk@zarz.agh.edu.pl, kubinski@agh.edu.pl

Впровадження інфосистем в галузі народного господарства, в яких здійснюється комерційний облік спожитих енергетичних ресурсів чи виготовленої продукції в формі дискретних одиниць за допомогою унітарного сумування, ставить жорсткі вимоги щодо завадозахисту інфопотоків в каналах зв'язку. Для цифрових каналів зв'язку характерні наступні типи помилок, що потенційно можуть виникнути в каналі зв'язку: інвертування цифрових значень бітів, наведення помилкових, або «випадання» інформативних. При цьому в системах з унітарним обліком досить рідко зустрічається перший і як основний можна визначити останній тип помилок. Такі помилки спричиняють в одному з випадків до обліку неіснуючих наведених повідомлень, в іншому – втрату інформативних, що є недопустимим в системах комерційного обліку, і що визначає актуальним завдання розробки завадозахищених методів інфообміну.

В сучасних інфосистемах комерційного обліку застосовують методи як параметричної, так і цифрової

модуляції, причому останні в силу вищого потенційного завадозахисту знаходять більш широке застосування. Розроблено метод цифрової модуляції повідомлень джерел з унітарним виходом за допомогою біторієнтованих рекурсивних кодових послідовностей Галуа класу циклічних, які характеризуються наскрізною логічною взаємозалежністю, що дозволяє в реальному часі здійснювати слідкування, виявлення та коректування помилок. Даний метод передбачає необхідність додаткової параметричної модуляції кожного із унітарних бітів з виходу джерела повідомлень двома додатковими ознаками – цифровими «1» та «0». Оскільки для одного і того ж модуля перерахунку кільця Галуа існують кілька векторів, що дозволяють генерувати послідовності максимальної довжини, вектори зворотного зв'язку пристрою кодування на стороні передачі повинні однозначно відповідати векторам декодерів на стороні прийому даних.

У порівнянні з унітарним кодуванням запропонований метод дозволяє визначати не тільки миттєву активність, але і сумарне значення параметру щонайменше на періоді слідування n бітів, що визначається модулем перерахунку N ($n=log_2N$). Така властивість дозволяє не тільки автоматично визначати помилку, але і здійснювати її автоматичне видалення з вхідного регістру із занесенням вірогідного значення без додаткових обчислювальних затрат. В доповіді наведено принципи кодування-декодування, схеми та алгоритми автоматичного виявлення та коректування помилок.

Розроблено та вперше запропоновано кодонний метод цифрової модуляції, що полягає у послідовній n-розрядно орієнтованій маніпуляції, який дозволив зменшити період ідентифікації сумарного значення джерела повідомлень до одного періоду слідування унітарних імпульсів.

УДК 621. 391

АНАЛІЗ ЕФЕКТИВНОСТІ ПЕРЕТВОРЕННІ ФОРМИ ІНФОРМАЦІЇ В СИСТЕМАХ КОДУВАННЯ ГАЛУА

Л.Б. Петришин (L. Petryshyn) проф., докт. техн. наук
Гірничо-металургійна академія м. Краків, Польща
(AGH University of Science and Technology Krakow, Poland)
petryshynl@poczta.fm, petryshynl@mail.ru

В.Вашкелевич (W.Waszkielewicz) проф., докт. техн. наук
Гірничо-металургійна академія м. Краків, Польща
(AGH University of Science and Technology Krakow, Poland)
waszkiel@zarz.agh.edu.pl

Однією із основних тенденцій при впровадженні сучасних інфотехнологій є побудова докладних математичних, алгоритмічних та програмних моделей об'єктів інформатизації, що визначає актуальним завдання значного покращення техніко-економічних параметрів засобів перетворення форми інформації (ПФІ) шляхом зменшення похибки перетворення чи збільшення кількості розрядів машинного слова, розширенням смуги частотного спектру чи підвищенням швидкодії перетворення, спрощенням структури засобів ПФІ, реалізацією послідовного інтерфейсу та завадозахищеного інфообміну. Оскільки екстенсивний шлях покращення параметрів засобів ПФІ обмежується технологічним рівнем електронного виробництва, вихід полягає у дослідженні та розробці нових методів кодування та ПФІ.

Аналіз сучасних тенденцій у методах ПФІ та характеристик систем кодування дозволив визначити, що системи кодування Галуа із рекурсивним впорядкуванням кодових елементів володіють одними із кращих показників

інформаційної потужності, що дозволяє зменшити кількість інформації, яка циркулює в інфомережі, підвищити швидкість інфообміну та ефективність використання каналів зв'язку, зменшити складність обчислювального середовища та затрати обчислювальної потужності, внаслідок чого зменшити кошти виготовлення та експлуатації інфотехнології.

Основною властивістю систем кодування Галуа є наскрізна логічна рекурсивна взаємозалежність кодових елементів, що дозволяє перейти від кодування кожного із повідомлень паралельними кодами до послідовного векторного біторієнтованого кодування масиву повідомлень шляхом ідентифікації кожного із повідомлень одиничним бітом Галуа.

Результати детального аналізу характеристик джерел повідомлень на нижньому мережному рівні дозволили класифікувати засоби ПФІ на перетворювачі, що здійснюють

- цифрову модуляцію послідовностями Галуа унітарних та частотно-імпульсних інфопотоків;
- аналого-цифрове перетворення неперервних в функції часу інфопотоків;
- аналого-цифрове перетворення параметрів типу переміщення та позиціонування в просторі.

В доповіді наведено основи здійснення вказаних процедур ПФІ на базі нових - скануючого, слідкуючого та імовірнісного методів, наведено структурні схеми та часові діаграми, що дозволяють підсумувати регулярну архітектуру, спрощення вихідного шифратора, підвищення швидкодії, реалізацію послідовного інтерфейсу та зменшення кількості вихідних шин і, як наслідок, зменшити вартість виготовлення. Визначено основні техніко-економічні показники, за якими здійснено оцінку ефективності застосування кожного із рішень.

УДК 681.32

УПРАВЛЯЕМАЯ СИНХРОНИЗАЦИЯ ДИНАМИЧЕСКИХ СИСТЕМ

А.М. Ковалев[1], чл.-корреспондент НАНУ,
А.Я.Савченко[2], чл.-корреспондент НАНУ,
В.Ф. Щербак[1], к.т.н., доцент
[1]ИПММ НАН Украины, [2]ИТК НАН Украины
e-mail: kovalev@iamm.ac.donetsk.ua

В последние десятилетия проводятся интенсивные исследования хаотических динамических систем для создания новых перспективных телекоммуникационных технологий. Свойством, позволяющем выделять информацию из шумоподобного сигнала хаотической системы передатчика является синхронизируемость их траекторий. В сообщении предлагается другой способ определения состояния передатчика, связанный с построением его динамического расширения и синтеза управлений, при которых алгебраические уравнения, связывающих искомый вектор состояния и решения принимающей системы, описывают инвариантное притягивающее многообразие.

Пусть динамика передатчика имеет вид

$$\begin{cases} \dot{x}_1 = f_1(t, x_1) + g_1(x_1)x_2, \\ \dot{x}_2 = f_2(t, x_1) + g_2(x_1)x_2,\ y = x_1 \end{cases}, \qquad (1)$$

где x_1 – передаваемый сигнал. Предположим, что правые части уравнений приемного устройства содержат произвольные функций $u_1(.) \in \mathrm{R}^k$, $u_2(.) \in \mathrm{R}^{n-k}$,

$$\begin{cases} \dot{p}_1 = f_1(t, x_1) + g_1(x_1)p_2 + u_1, \\ \dot{p}_2 = f_2(t, x_1) + g_2(x_1)p_2 + u_2 \end{cases}. \qquad (2)$$

Функции u_1 (.), u_2 (.) могут зависеть лишь от известных величин x_1 (t) и фазового вектора системы (2) -- координат $p_1(t)$, $p_2(t)$. Обозначим $e_i = p_i - x_i$, i=1,2. Уравнения для отклонений траекторий систем имеет вид

$$\begin{cases} \dot{e}_1 = g_1(x_1)e_2 + u_1, \\ \dot{e}_2 = g_2(x_1)p_2 + u_2 \end{cases}. \qquad (3)$$

Будем рассматривать задачу определения переменных x_2 как задачу построения дополнительных n-k алгебраических уравнений вида

$$e_2 - \Phi(x_1, e_1) = 0. \qquad (4)$$

Тогда для решения задачи достаточно подобрать управления $u_1(.)$, $u_2(.)$ так, чтобы для траекторий расширенной системы (1), (2) или, что то же самое – системы (1), (3), выполнялось условие: равенства (4) описывали инвариантное многообразие, которое обладает свойством глобального асимптотического притяжения.

Предлагается двухэтапный метод синтеза. На первом шаге решается задача синтеза управлений, делающим произвольно заданное гладкое многообразие (дополнительный выход) инвариантным для системы (1),(3). Вид многообразия (функция $\Phi(x_1, e_1)$) выбирается на втором этапе как решение уравнений в частных производных для обеспечения свойства глобального притяжения траекторий расширенной системы. Как пример, рассматриваются уравнения Эйлера

$$\dot{x}_1 = \frac{A_2 - A_3}{A_1} x_2 x_3, \quad \dot{x}_2 = \frac{A_3 - A_1}{A_2} x_1 x_3, \quad \dot{x}_3 = \frac{A_1 - A_2}{A_3} x_1 x_2$$

и строится их управляемый аналог. Функция

$$\Phi = -\sqrt{\frac{A_1 A_2}{(A_3 - A_1)(A_3 - A_2)}} arctg\left(\sqrt{\frac{(A_3 - A_1)A_1}{(A_3 - A_2)A_2}} \cdot \frac{x_1}{x_2} \right).$$

определяет инвариантное, глобально притягивающее многообразие $e_3 - \Phi(x_1, x_2) = 0$.

УДК 519.711/.72

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ПРЕОБРАЗОВАНИЙ ГРЕЯ

А.Я.Белецкий, д. т. н, профессор
Национальный авиационный университет,
e-mail: abelnau@ukr.net

Коды Грея, предложенные в середине XX века в ответ на запросы инженерной практики относительно построения оптимальных по критерию минимума ошибки неоднозначности преобразователей типа “угол–код”, на заре своего появления привлекли к себе внимание не только исследователей математиков, но и широкого круга разработчиков разнообразной аппаратуры. Отличительная особенность кодов Грея состоит в том, что в двоичном пространстве (или в двоичной системе счисления) при переходе от изображения одного числа к изображению соседнего старшего или соседнего младшего числа происходит изменение цифр (1 на 0 или наоборот) только в одном разряде числа..

За пятидесятилетнюю историю своего развития теория кодов Грея претерпела незначительные изменения. По-видимому, оказались вне поля зрения как математиков, так и разработчиков аппаратуры возможности построения кодов, *инверсных* по направлению формирования *классическим* кодам Грея. В известной схеме процесс формирования прямых и обратных кодов Грея развивается слева направо. Вместе с тем можно построить схему преобразования m-ичных кодов, обратную по направлению классическому (*левостороннему*) преобразованию Грея. В таком классе преобразований, который назван

правосторонним, при прямом и обратном преобразованиях сохраняется неизменным значение младшего (правого) разряда преобразуемого числа.

Комбинация лево- и правостороннего преобразования по Грею (как прямого, так и обратного) совместно с операцией инверсной перестановки послужила основой построения комбинированных или *составных* кодов Грея. Применение составных кодов оказалось весьма успешным в задачах определения структуры и взаимосвязи базисных симметрических систем Виленкина-Крестенсона функций (ВКФ), частным случаем которых являются системы функций Уолша. И, тем не менее, не для всех порядков систем ВКФ удается «связать» полное множество систем. Возникает так называемая проблема *кластеризации*, которая, для примера, проявляется в том, что только 128 из 448 систем функций Уолша 16-го порядка оказалось возможным синтезировать с помощью *простых* кодов Грея. Обозначенную проблему кластеризации удалось разрешить введением *обобщенных* кодов Грея.

В докладе обсуждаются теоретические основы построения алгебраической системы (*группы преобразования Грея*), состоящей из конечного числа элементов (так называемых *индикаторных матриц* систем ВКФ), на множестве которых определена бинарная операция типа умножения, удовлетворяющая следующим основным аксиомам: операция ассоциативна; гарантирует единицу и обратные элементы; замкнута для каждой пары элементов, входящих в группу.

Рассматриваются различные направления применения разрабатываемых преобразований.

УДК 681.3:519.62

ЗАСТОСУВАННЯ ДВОСТУПЕНЕВОЇ МОДУЛЯЦІЇ ІЗ ВИПАДКОВИМ НЕСУЧИМ СИГНАЛОМ ДЛЯ ПЕРЕДАЧІ ЦИФРОВОЇ ІНФОРМАЦІЇ

С.Б.Приходько, к.т.н., доцент
Національний університет кораблебудування
e-mail: sbp@usmtu.edu.ua

В останні роки з метою покращення властивостей систем передачі цифрової інформації робляться спроби застосування у якості несучої негармонійні сигнали, в тому числі і випадкові. Їх використання дає змогу покращити як захищеність інформації, яка передається, так і завадостійкість системи передачі. У 1999 році A.-B.Salberg та A.Hansen вперше ввели поняття так званої маніпуляції випадкового процесу (stochastic process shift keying, SPSK), при якій на заданому часовому інтервалі один випадковий процес задає біт нуль, а інший випадковий процес задає біт одиниця. Вони запропонували застосовувати SPSK для захисту інформації, яка передається, а у якості випадкових процесів використовувати процеси авторегресії ковзняного середнього і показали її реалізацію на прикладі двох процесів авторегресії третього порядку. Отримані ними результати с точки зору відношення енергії інформаційного сигналу, яка припадає на один біт, що передається, до енергії шуму E_b/E_n виявилися слабкими: всього 20 дБ при ймовірності появи бітової похибки 10^{-5}. Пізніше автором цих тез було запропоновано створювати несучі інформацію випадкові процеси (сигнали) за допомогою стохастичної диференціальної системи (СДС). При цьому через параметри СДС у випадковий процес

підмішуються дані і синхросигнал. Детектування даних в приймачеві здійснюється за прийнятим випадковим сигналом на основі двох основних процедур: процедури розпізнавання синхросигналу (визначення моменту зміни параметрів СДС, які задають інформацію) та процедури детектування інформації (оцінки параметрів СДС). У якості першої процедури було запропоновано використовувати дискриминантну процедуру, яка базується на порівнянні імовірнісних характеристик випадкового процесу у двох сусідніх часових вікнах. Друга процедура – оцінки параметрів СДС або параметричної ідентифікації СДС, спочатку була побудована на основі метода моментів, а пізніше – на основі узагальненого методу моментів. З часом була показана практична реалізація запропонованого способу передачі даних при впливі на випадковий сигнал у каналі зв'язку широкосмугових завад до значень відношення енергії сигналу до енергії шуму, рівних $-0{,}5$ дБ. Випадкові процесів, які створені за допомогою СДС, у принципі можуть використовуватися у якості інформаційних несучих сигналів безпосередньо у каналі зв'язку. Але враховуючи на те, що зараз краще розвинуті традиційні методи модуляції, доцільним було б застосувати двоступеневу модуляцію: на першій стадії виконувати SPSK, а на другій – здійснювати модуляцію отриманого на першій стадії випадкового процесу одним із традиційних методів. В даній роботі для цього пропонується використовувати квадратурну амплітудну модуляцію (quadrature amplitude modulation, QAM). Розроблено спосіб передачі цифрової інформації із застосуванням SPSK та QAM. Показано, що така двоступенева модуляція дає змогу, по-перше, зменшити відношення E_b/E_n до значень менших за $-1{,}6$ дБ, а, по-друге, покращити захист інформації, яка передається.

УДК 621.391.019.3

ХАРАКТЕРИСТИКИ ЗГОРТКОВИХ КОДІВ ДЛЯ СИСТЕМ З ПРОСТОРОВО-ЧАСОВИМ КОДУВАННЯ

М.О. Іщенко, викладач
Одеська національна академія зв'язку ім. О.С. Попова
e-mail: dima_ischenko@rambler.ru

Однієї з основних цілей впровадження систем безпроводового зв'язку є надання абонентові послуг широкосмугового доступу. Передача мультимедійних повідомлень у реальному масштабі часу вимагає великих швидкостей, у десятки разів перевищуючі швидкості в існуючих системах мобільного зв'язку. Методи просторово-часового кодування (ПЧК) забезпечують кращий обмін між частотною і енергетичною ефективністю та прийняті до уваги при формуванні стандартів третього покоління систем мобільного радіозв'язку (CDMA-2000, W-CDMA) та інших служб безпроводового доступу. Ефективним методом боротьби з завмираннями в каналах радіозв'язку є рознесення, при якому утвориться кілька різних шляхів проходження сигналу від передавача до приймача. Традиційні методи, засновані на використанні рознесених прийомних антен з наступним комбінуванням прийнятих сигналів, але не можуть бути застосовані в системах мобільного зв'язку. Основна увага в останні роки приділяється методам, коли інформація до абонента передається через декілька рознесених у просторі передавальних антен, причому сигнали різних антен піддаються спеціальному кодуванню. Такі просторово-часові коди дають виграш по завадостійкості в каналах із завмираннями як за рахунок

кодування, так і за рахунок рознесення каналів передачі.

Просторово-часове кодування розглядається як перспективна альтернатива при виборі методів передачі інформації в системах безпроводового доступу як для фіксованого так і для мобільного зв'язку.

Незважаючи на велику актуальність метода ПЧК у вище сказаному, відсутні відомості про характеристики згорткових кодів (дані про породжуючі поліноми, наприклад). Аналіз показав, що в системах ПЧК доцільно використати недвійкові згорткові коди та багатопозиційну фазову модуляцію (ФМ-М) у вигляді оптимального сполучення ансамблів сигналів з високою питомою швидкістю й оптимальних, погоджених з ними згорткових кодів. Для рішення цього завдання автором розроблено алгоритм переборного пошуку оптимальних породжуючих поліномів згорткових кодів. Програма реалізації даного алгоритму переборного пошуку, розроблена мовою С++, з використанням пакета візуального об’єктного програмування *HP VEE*. На основі даного методу знайдені нові породжуючі поліноми оптимальних кодів.

Автором пропонуються характеристики нових згорткових кодів для систем з просторово-часовим кодування з використанням багатопозиційною фазовою модуляцією. Проведено аналіз ефективності найдених просторово-часових кодів.

Знайдені просторово-часові коди рекомендуються автором для впровадження в проектування перспективних систем безпроводового доступу мереж загального користування.

УДК 004.052.32

ОЦЕНКА ЭФФЕКТИВНОСТИ КОНТРОЛЯ ОШИБОК В БИНОМИАЛЬНЫХ ЦИФРОВЫХ УТРОЙТВАХ

В. В. Гриненко
Сумский государственный университет
grvital@list.ru

Одним из способов повышения достоверности функционирования цифровых устройств является введение избыточности, позволяющей обнаруживать возникающие ошибки, за счет изменения первичного представления чисел с использованием помехоустойчивых кодов. Однако при этом необходимо проводить оценку эффективности применения кодов. Поэтому актуальной является задача по оценке эффективности контроля цифровых устройств построенных на основе биномиальных двоичных кодов.

Для оценки использовался метод учитывающий вероятность необнаружения ошибки на выходах устройства. В качестве модели ошибок, на основе анализа литературы, было предложено разделить возникающие ошибки по степени кратности, так как в цифровых устройствах преобладают однократные, двукратные и трехкратные ошибки. Для определения количества необнаруживаемых ошибок биноммиальный код с параметрами n и k был разбит на $k+1$ подмножество по числу единиц в кодовой комбинации. Были получены соотношения, позволяющие определять какой процент ошибок определенной кратности не контролируется заданным биномиальным кодом. На основе полученных выражений можно производить оценку эффективности применения различных биномиальных кодов.

УДК 681.32

АНАЛІЗ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ ПЕРЕТВОРЕННЯ ГАНКЕЛЯ ПРИ ЗАВАДОЗАХИЩЕНОМУ ІНФООБМІНІ

Н. В. Превисокова, асистент
Прикарпатський національний університет
імені Василя Стефаника
e-mail: natvolo@rambler.ru

Інтенсивний розвиток та впровадження інфотехнологій зумовлює необхідність застосування нових підходів у реалізації процедур інфообміну та цифрової обробки повідомлень, що вимагає забезпечення достовірності даних із використанням процедур завадостійкого кодування. Завадостійкість і швидкість передавання інформації залежить як від характеристик каналу так і від методів кодування та декодування. Широкого застосування в практиці завадостійкого кодування набули методи алгебраїчного кодування лінійних блокових кодів, проте недостатньо обґрунтовано застосування кодових систем Галуа для реалізації процедур кодування в полі раціональних чисел, що зумовило актуальність досліджень.

В процесі кодування вхідна інформаційна послідовність довільних раціональних чисел поділяється на блоки $Q=(Q_1, Q_2,..., Q_k)$, і кожний блок доповнюється перевірними символами ρ_j, $j=1,...,m$. У лінійних блокових кодах перевірочні символи є лінійними функціями від інформаційних символів $Q_1, Q_2,..., Q_k$, а кодове слово $U=\{Q_1, Q_2,..., Q_k, \rho_1, \rho_2,..., \rho_m\}$ визначається як скалярний добуток $U=QG$ інформаційного вектора Q на породжуючу

матрицю G, яка подається у стандартній систематичній формі $G=[E|G_1]$ де E – одинична діагональна матриця, G_1 - матриця, рядки якої лінійно незалежні. Для перевірки векторів повідомлень будується перевірочна матриця H, ортогональна до породжуючої G згідно $H=[H_1|E]$.

Результати проведених досліджень визначили ефективність використання в якості породжуючої матриці дискретних значень функцій системи Галуа, яка є ганкелевим циркулянтом $G_1=G_ц$. Формування послідовностей дискретних значень функцій Галуа здійснюється за допомогою відповідного породжуючого вектора елементів поля Галуа $GF(2^n)$. Операції кодування $U=QG$ та перевірки повідомлень $UH^T=0$ реалізуються внаслідок перемноження вектора на циркулянти $G_ц$ та $H_1=H_ц$. Якщо G – Ганкелева матриця, Q – n-вимірний вектор, то для знаходження QG достатньо виконати $K\leq C\cdot n\ log_2 n$ арифметичних операцій, де $C>0$, яке позначається як $O(n\ log_2 n)$. Таким чином, використання в якості породжуючої та перевірочної матриць ганкелевих циркулянтів Галуа дозволило зменшити обчислювальну складність процедур кодування та перевірки повідомлень від $O(n^2)$ до $O(n\ log_2 n)$.

При прийомі цифрового повідомлення з метою виявлення та виправлення помилок використовується синдромний метод декодування. На основі аналізу структури перевірочної матриці циркулянта розроблено алгоритм декодування, який базується на елементарних перетвореннях матриці H і дозволяє уникнути розв’язування рівняння локаторів та системи нелінійних рівнянь для визначення позицій помилок, що спрощує процедуру декодування.

УДК 681.3

ВИКОРИСТАННЯ ХАРАКТЕРИСТИК ПЕРВИННОГО КОДУ ДЛЯ ПОБУДОВИ КОДІВ, ЩО ЗНАХОДЯТЬ ТА ВИПРАВЛЯЮТЬ ПОМИЛКИ

В. А. Лужецький, д.т.н., професор
Вінницький національний технічний університет

Відомі методи завадостійкого кодування описують побудову лінійного або нелінійного коду для повідомлення, що складається з повного набору символів. При цьому блок з k символів повідомлення (первинний код) $\mathbf{u} = u_1 u_2 ... u_k$ $(u_i = \{0;1\})$ перетворюється в кодове слово $\mathbf{x} = x_1 x_2 ... x_n$ $(x_j = \{0;1\}, n > k)$. Набір кодових слів утворює завадостійкий код, кожне кодове слово якого має задовольняти рівнянню:

$$\mathbf{H}\mathbf{x}^T = 0,$$

де **H** – перевірочна матриця.

Теоретично можливо побудувати матрицю **H** таку, щоб вона забезпечувала певні характеристики завадостійкого коду. Однак ця матриця може виявитися занадто складною для практичної реалізації процесу кодування. Тому шукають певні підходи, які можуть спростити процес кодування.

У доповіді розглядається підхід, що базується на врахуванні характеристик первинного коду h(**u**).

Пропонуються такі схеми побудови кодових слів:

$$\mathbf{x} = \mathbf{u} \,||\, K\big(h(\mathbf{u})\big); \quad (1)$$

$$\mathbf{x} = F\big(h(\mathbf{u}), P\big), \quad (2)$$

де $K\big(h(\mathbf{u})\big)$ код характеристики; P –параметр.

Набір символів $u_1 u_2 .. u_k$ можна розглядати як

послідовність незалежних символів або як код певного математичного об‘єкта .

Послідовність незалежних символів може характеризуватися або кількістю одиниць n для всього первинного коду, або кількістю одиниць n_i для певних груп розрядів цього коду. Тому маємо такі характеристики:

$$h_{\text{код}}(\mathbf{u}) = n;\ h_{\text{код}}(\mathbf{u}) = n \bmod m,\ m \geq 2;$$

$$h_{\text{гр}i}(\mathbf{u}) = n_i;\ h_{\text{гр}i}(\mathbf{u}) = n_i \bmod m.$$

Прикладами відомих завадостійких кодів, побудованих за схемою (1) з використанням наведених характеристик, є коди з кодовим контролем за модулем та ітеративні коди.

Якщо первинний код розглядати як код математичного об‘єкта, то таким об‘єктом може бути число або поліном. При цьому характеристика визначається як функція $h(\mathbf{u}) = f(u_i, w_i)$, де w_i - математичний об‘єкт. Виходячи з цього, маємо такі варіанти:

$$h(\mathbf{u}) = u_k x^{k-1} + u_{k-1} x^{k-2} + \cdots + u_2 x + u_1;$$

$$h(\mathbf{u}) = \sum_{i=1}^{k} u_i s^{i-1},\ s - \text{ціле число};\quad h(\mathbf{u}) = \left(\sum_{i=1}^{k} u_i s^{i-1} \right) \bmod m;$$

$$h(\mathbf{u}) = \sum_{i=1}^{k} u_i w_i;\ h(\mathbf{u}) = \left(\sum_{i=1}^{k} u_i w_i \right) \bmod m,\ h(\mathbf{u}) = \prod_{i=1}^{k} u_i w_i$$

де $w_{i+g} = a_g w_{i+g-1} + a_{g-1} w_{i+g-2} + \cdots + a_1 w_i$ для початкових значень $w_1, w_2, ..., w_g$, a_j - цілі числа, w_i або цілі числа, або прості числа, або незвідні поліноми.

Прикладами відомих завадостійких кодів, побудованих за схемами (1) і (2), є коди з числовим контролем за модулем, коди Бергера, AN – коди та циклічні коди.

УДК 681.32

ДЕКОДИРОВАНИЕ КОДОВ РИДА-СОЛОМОНА ПО ГРАФОВЫМ МОДЕЛЯМ

В. П. Семеренко, к.т.н., доцент
Винницкий национальный технический университет
e-mail: sm@vinnitca.com

Код Рида-Соломона (РС) может быть задан с помощью математического аппарата линейной последовательностной машины (ЛПМ), которая над полем Галуа $GF(q)$ определяется как автомат Мура с функцией состояний (переходов)

$$S(t+1) = A \times S(t) + B \times U(t)$$

и функцией выходов

$$Y(t) = S(t),$$

где $U(t), Y(t), S(t)$ – векторы входной, выходной и состояний; A, B – характеристические матрицы вида

$$A = \begin{vmatrix} 0 & 0 & \cdots & 0 & \alpha_0^i \\ \alpha^0 & 0 & \cdots & 0 & \alpha_1^i \\ 0 & \alpha^0 & \cdots & 0 & \alpha_2^i \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \alpha^0 & \alpha_{2t-1}^i \end{vmatrix}, \quad B = \begin{vmatrix} \alpha^0 \\ 0 \\ 0 \\ \cdots \\ 0 \end{vmatrix}, \; i = 0,1, \ldots 2^m - 1 \; .$$

Элементы последнего столбца матрицы A представляют собой коэффициенты порождающего полинома кода РС

$$g(x) = \alpha_0^i + \alpha_1^i X + \alpha_2^i X^2 + \ldots + \alpha_{2t-1}^i X^{2t-1} + X^{2t} \, .$$

Графовой моделью такой ЛПМ является ориентированный граф $G(V, E)$ следующей структуры.

Имеется тривиальный нулевой цикл (ТНЦ), состоящий из одной вершины, и совокупности периферийных нулевых циклов (ПНЦ) длины $(q-1)$, которые можно расположить по t уровням. Каждая вершина графа из множества V соответствует состоянию автомата Мура, а дуги из множества E обозначают переходы между состояниями после подачи на автомат соответствующих входных воздействий. С ТНЦ связан i-й НПЦ первого уровня с помощью дуги α^i, а каждый h-й ПНЦ j-го уровня связан с одним ПНЦ $(j-1)$-го уровня с помощью дуги α^h. Внутри каждого ПНЦ вершины связаны между собой с помощью нулевых дуг.

Задача исправления ошибок в коде РС по его графу $G(V, E)$ сводится к поиску пути от вершины, соответствующей синдрому ошибки, к ТНЦ. Для уменьшения трудоемкости вычислений предлагаются новые компактные графовые модели, в которых учитывается только минимальное количество переходов между ПНЦ соседних уровней по связывающим вершинам. Для сокращения времени поиска пути можно параллельно искать фрагменты пути внутри ПНЦ разных уровней.

Аналитически процедура декодирования полученного из канала связи кодового вектора $C(x)$ сводится к последовательному вычислению по формуле (1) векторов состояний ЛПМ той же структуры, которая использовалась при кодировании этого кодового вектора.

Предлагаемые графовые модели позволяют более глубоко исследовать корректирующие способности кодов РС а также обнаруживать и исправлять большее количество ошибок по сравнению с известными методами.

УДК 519.725

КЛАСИФІКАЦІЙНА МОДЕЛЬ ОДИНИЧНИХ КОДІВ

Т. Б. Мартинюк, к.т.н., доцент,
А. Г. Буда, к.т.н., доцент,
Н. В. Фофанова, методист
Вінницький національний технічний університет
e-mail: oeipt@vstu.vinnica.ua, natfo@ukr.net

Відомо, що завадостійкі коди широко застосовуються не тільки при передачі даних з метою виявлення та виправлення помилок, але й при кодуванні станів мікропрограмних автоматів у пристроях управління та при адресації інформації у запам'ятовуючих пристроях обчислювальної техніки. Так, доведена доцільність використання одиничного кодування станів мікропрограмних R-автоматів (RA) для граф-схем алгоритмів зі значно розгалуженою структурою.

Одиничне кодування в цьому випадку дозволяє не тільки зменшити складність логічного перетворювача, але й спростити процес синтезу RA, який реалізується на паралельно-послідовних (зсувних) регістрах. Збільшення складності запам'ятовуючої частини RA, яке виникає при цьому, легко реалізується при використанні ПЛІС.

У роботі зроблено аналіз двох різновидів одиничного коду, а саме одиничного позиційного і одиничного нормального кодів з погляду класичної теорії кодування. Показано місце цих кодів у відомій класифікаційній моделі кодів. Порівняльний аналіз одиничних кодів виконано за такими ознаками як лінійність, циклічність, надлишковість, подільність, систематичність, еквідістатність, рівномірність,

рівноважність.

Для цього було використані такі поняття алгебраїчної теорії кодування, як матриця кодування, блокова довжина, перевірочна матриця, синдром, кодова попарна відстань, вага слова, суміжний клас, лідер, які дозволяють не тільки класифікувати код, але й визначити його завадостійкість та контролездатність.

Аналіз характеристик одиничного позиційного і одиничного нормального кодів з точки зору їх контролездатності показав, що вони відносяться до нелінійних кодів, але для них існує можливість складання відповідних модифікованих перевірочних матриць, що в свою чергу, дозволяє виконати синдромне декодування отриманого коду з виявленням помилок і навіть з можливістю виправлення помилок за певної умови в одиничному нормальному коді.

Отже, надлишковість інформаційних позицій (розрядів) в обох одиничних кодах по відношенню до двійково-десяткових кодів призводить до підвищення рівня реальної контролездатності у порівнянні з теоретичною, оскільки вони складають клас нелінійних кодів. Крім того, обидва одиничні коди мають просте синдромне декодування (за аналогією з кодом Хеммінга), оскільки відхилення у позиціях (розрядах) сформованого синдрому у порівнянні з правильним синдромом для кожного з двох одиничних кодів вказує на конкретну помилкову позицію у прийнятому слові.

За результатами порівняльного аналізу одиничних кодів їх можна класифікувати як окрему групу кодів зі специфічними властивостями.

УДК 681.3

КОДИРОВАНИЕ ВЕСОВЫХ КОЭФФИЦИЕНТОВ В СОРТИРУЮЩЕЙ НЕЙРОСЕТИ

Т.Б.Мартынюк, к.т.н., доцент,
Мохамед Салем Нассер, аспирант,
Л.В.Огороднийчук
Винницкий национальный технический университет
oeipt@vstu.vinnica.ua

Для нейросетевых архитектур определяющим является не только способ обучения, но и вид матрицы весовых коэффициентов (МВК) в начале или по завершению процесса обучения. Так, например, после обучения нейросети типа ДАП (двунаправленная ассоциативная память) МВК содержит положительные значения элементов главной диагонали и отрицательные значения остальных элементов.

В предложенной сортирующей нейросети (S-нейросети), реализующей метод сортировки парным обменом с подсчетом, МВК перед обучением имеет вид единичной матрицы. В процессе обучения такой нейросети происходит изменение весовых коэффициентов, которые в данном случае представляют собой ранги соответствующих элементов входного векторного массива чисел. При этом особенностью изменения весовых коэффициентов является увеличение (уменьшение) на единицу значений соседних весов, то есть фактически реализация операций инкремента (декремента).

Таким образом, одним из вариантов задания рангов элементов входного массива чисел, размерностью n, является натуральный ряд чисел 1,…,n, представленных в

виде единичного позиционного кода. Этот код является нелинейным избыточным пространственно-распределенным кодом, который с учетом возможностей современных технологий (ПЛИС и оптоэлектроника) хорошо зарекомендовал себя при синтезе устройств управления (процедура кодирования состояний микропрограммных автоматов) и при реализации ассоциативных процессоров (адресация по содержанию).

В работе рассмотрены особенности единичного позиционного кодирования чисел, а также выполнен сравнительный анализ аппаратных и временных затрат при использовании единичного позиционного и двоичного кодов для представления рангов (весов) при сортировке векторного массива чисел.

УДК 681.32

QUANTUM TIME LENGHTH ESTIMATION FOR ROUND-ROBIN SCHEDULING ALGORITHM USING NEURAL NETWORKS

Omar AlHeyasat, Associate Professor
Mu'tah University 61710, Karak, Jordan
e-mail: omarah@mutah.edu.jo

In Round Robin (RR) scheduling algorithm that used for CPU scheduling is considered the fairness compromise algorithm among different mechanisms and disciplines that deals with sharing the CPU time between processes that resides in the ready queue. RR, First come first served, high priority, shortest job first and other algorithms have several disadvantages when dealing with real-time systems and deadline limitations. In real-world of time-sharing systems, RR service (behavior) is widely used. Many publications discussed the RR scheduling algorithm, its efficiency, reliability, and its consistency if it was apart of a general system. Ramabhadran et al presented analytical and simulation results based on RR algorithm in a manner of a stratified RR scheduler. Jorge R. et al showed a modified RR algorithm that predicts potential job departures and schedules them in advance. John Tsiligaridis et al discussed a very important algorithm that constitutes an alternative way of defining the most suitable size of the quantum in RR scheduling algorithm using gradual or direct weight increase mechanisms, and in the same paper the author strongly stated that this kind of algorithms can be applied for next generation internet routers. Seungmin Baek et al in described a packet filtering-based RR scheduling scheme for tightly coupled clusters in terms of throughput and reliability.

Rahul Garg et al in described a scheduling algorithm named recursive round robin scheduler (RRR), based on the concept of the construction of scheduling tree, and showed that the work conserving scheduler is fair. While Salil et al used a technique to analytically derive the latency bound of pre-ordered DDR. Many other publications describes, discussed, and proved many scheduling algorithms, almost in all publications, authors selected different criteria, like fairness, bounded delay, low complexity, deadline and other criteria.

It is evident that the performance of the RR scheduling algorithm is highly interrelated to the length of the quantum time. Therefore, the impact of contributing variables on the length of the quantum time is uncertain and complex. Under such circumstances, artificial intelligence techniques such as neural networks are known as an outstanding prediction tools. The major objective of this study is to develop a handy formula for estimating the length of the quantum time that should be used on the RR scheduling algorithm when dealing with different types of jobs (mix job problem) instead of taking the quantum time length as a fixed value in almost all applications that uses RR. Two techniques are used in preparing the prediction formula, namely linear regression (LR) and neural networks (NNT). The data that was used in this paper includes 10,000 data sets, each data set includes 10 random numbers which are the expected service time, each data set was observed 50 times, when the quanta were 0.1, 0.2, 0.3, …, 4.8, 4.9, 5.0 units of time. After each run, the average turnaround time and the average waiting time were moved into appropriated cell in the output excel data sheet. It was shown that it efficient to use the neural networks to estimate the quantum time length for Round Robin scheduling algorithms instead of considering it as fixed value.

УДК 621.391.2

ФАКТОРИЗАЦІЯ МАТРИЦЬ УОЛША

О.А. Кожухівська
Київський національний авіаційний університет

Використання кронекеровського добутку матриць, а також кронекеровського добутку матриць по рядкам і стовпцям дозволяє розглянути ряд факторизацій матриць Уолша.

Нехай $N = 2^n$, де n - натуральне число. Матрицю Уолша-Адамара можна представити у вигляді:

$$\mathbf{H}_h(N) = \prod_{j=1}^{n} \left\{ \mathbf{E}_{2^{(j-1)}} \otimes \left[\mathbf{H}(2) \otimes \mathbf{E}_{2^{(n-j)}} \right] \right\}; \qquad (1)$$

$$\mathbf{H}_h(N) = \prod_{j=1}^{n} \left\{ \mathbf{E}_{2^{(n-j)}} \otimes \left[\mathbf{H}(2) \otimes \mathbf{E}_{2^{(j-1)}} \right] \right\}; \qquad (2)$$

$$\mathbf{H}_h(N) = \left[\mathbf{E}_{2^{(n-1)}} \overline{\otimes} \mathbf{H}(2) \right]^n; \qquad (3)$$

$$\mathbf{H}_h(N) = \left[\mathbf{E}_{2^{(n-1)}} \widetilde{\otimes} \mathbf{H}(2) \right]^n, \qquad (4)$$

де $\mathbf{E}_{2^{(j-1)}}$ - одинична матриця порядку $2^{(j-1)}$,

$\otimes$ - кронекеровський добуток матриць,

$\overline{\otimes}$ і $\widetilde{\otimes}$ - кронекеровський добуток матриць по рядкам і по стовпцям відповідно,

$\mathbf{H}(2)$ - стандартна матриця Уолша-Адамара другого порядку.

У відношенні факторизацій (1) – (2) можна зробити зауваження, які будуть використані в подальшому.

Комутативність факторизацій матриць Уолша-Адамара згідно виразів (1) і (2) можна довести, використовуючи відому властивість симетричних матриць: добуток **C**=**AB** симетричних матриць **A** і **B** є симетричним, якщо **C** = **BA**, а також той факт, що матриця Уолша-Адамара симетрична.

Симетричність матриць ітерацій виразів (1) і (2) випливає із властивості кронекеровського добутку матриць: $(\mathbf{A} \otimes \mathbf{B})^t = \mathbf{A}^t \otimes \mathbf{B}^t$, де t - символ транспонування матриць.

Від виразу (3) до виразу (4) можливо перейти шляхом транспонування матриць ітерацій. Це випливає із властивості узагальненого кронекеровського добутку матриць: $(\mathbf{A} \overline{\otimes} \mathbf{B})^t = \mathbf{A}^t \widetilde{\otimes} \mathbf{B}^t$ і симетричності матриць Уолша-Адамара.

Вираз (2) співпадає з відомим алгоритмом Кулі-Тьюкі.

Матриці ітерацій згідно виразам (3) і (4) співпадають з відомими матрицями ітерацій, що приведені в літературі, проте досяжні більш простим шляхом, а також дозволяють отримати правила побудови ортогональних дискретних функцій для будь-якого $N \geq 1$. Це буває необхідно при використанні систем функцій Уолша, коли кількість відліків послідовностей $N \neq 2^n$.

Висновок. Алгоритми факторизації матриць Уолша-Адамара згідно виразам (1) і (3) зручні для реалізації їх в реальному масштабі часу, оскільки для початку обчислення спектральних коефіцієнтів достатньо мати на вході два перших відліки вхідного сигналу. Вони є також зручними для реалізації в векторному режимі для комп'ютерів типу "одна команда – багато даних".

2. Методи та засоби захисту інформації

УДК 681.324.067

КЛАСТЕРНЫЙ ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ СУПЕРКОМПЬЮТЕРНОГО ЦЕНТРА

В.В. Анищенко, доцент,
В.И. Стецюренко, к.т.н., с.н.с., А.М. Криштофик,
Объединенный институт проблем информатики
НАН Беларуси,
e-mail: witas@newman.bas-net.by

В Объединенном институте проблем информатики создан и функционирует «***Республиканский суперкомпьютерный центр коллективного пользования» (РСКЦ КП),*** который объединяет вычислительные мощности суперкомпьютерных конфигураций «СКИФ»: кластеры К-500 и К-1000 (соответственно 128 и 576 процессоров с Linpack-производительностью К-1000 - 2.0 Тфлопс).

Кластеры РСКЦ КП по оптоволокну подключены к FDDI-кольцу Академсети «BASNET», к которой, в свою очередь, через сетевое оборудование подключаются многочисленные абоненты (учреждения НАН Беларуси, предприятияи и организации – пользователи РСКЦ КП, расположенные в г.Минске).

Удаленным пользователям вычислительные ресурсы кластеров в реальном времени предоставляются через сеть «BASNET» и транспортную сеть ИНТЕРНЕТ, что предопределяет существование для ресурсов РСКЦ КП угроз безопасности, присущих сетям общего пользования.

По сведениям зарубежных источников наблюдается значительное увеличение атак именно на

суперкомпьютерные центры, так как в них сосредоточены огромные информационные ресурсы и в случае успешной атаки злоумышленник получает доступ к этим ресурсам.

По этой причине было принято решение о выделении РСКЦ КП в отдельный сегмент защиты и администрирования безопасности с использованием персонального средства – программно-аппаратного комплекса (ПАК) с интеграцией различных сервисов безопасности (аутентификации, межсетевого экранирования обнаружения вторжений, антивирусной защиты, мониторинга и аудита, управления и администрирования) в совокупности с построением такого комплекса на принципах кластерных технологий с распараллеливанием обработки.

Кластер ПАК включает в себя 5 узлов, один из которых является управляющим, на управляемых узлах реализуется параллельная обработка входящего трафика и реализуются функциональные требования безопасности.

Для конфигурирования ПАК, просмотра и анализа данных аудита и реализации задач администрирования в состав ПАК включено автоматизированное рабочее место администратора безопасности.

Программное обеспечение ПАК: встроенная операционная система (ВОС) на базе ядра ОС Linux, специализированное ПО, функционирующее в среде ВОС.

Принятые архитектурные и технологические решения как параллельная обработка трафика и одновременный анализ нескольких соединений обеспечивают такие свойства ПАК как высокая производительность и масштабируемость, надежность и отказоустойчивость, оптимальное соотношение стоимости системы защиты к стоимости защищаемого объекта.

УДК 004.056

УДК 681.3

ЕКСПЕРТНА СИСТЕМА ДЛЯ ПІДТРИМКИ КЕРУВАННЯ БЕЗПЕКОЮ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

В.П.Тарасенко, д.т.н., професор,
А.Ю.Михайлюк, к.т.н., доцент,
А.В.Петрашенко, ст. викладач
Національний технічний університет України
"Київський політехнічний інститут"
e-mail: may@scs.ntu-kpi.kiev.ua

Керування безпекою комп'ютерних систем за класичним означенням належить до числа задач, структурування і формалізація яких ускладнена. Виходячи з цього ефективним засобом інструментальної підтримки вказаного процесу є експертна система.

У доповіді запропоновано структурно-алгоритмічну організацію спеціалізованої експертної системи для аналізу захищеності комп'ютерної системи та оптимізації відповідної комплексної системи захисту інформації (КСЗІ). База знань експертної системи може формуватись на основі відповідних нормативних документів, а також акумулювати особистий досвід експертів. Критерій оптимізації КСЗІ враховує зокрема власне рівень захищеності, вартість створення КСЗІ, поточні витрати на його утримання тощо, причому питома вага перелічених чинників може обиратися користувачем. Доповідь містить опис структури бази знань та алгоритми відповідних механізмів виведення, узагальнену методику формування бази знань та організацію автоматизованих робочих місць експертів. Наводяться результати експериментального впровадження прототипу експертної системи.

УДК 681.32

ОБРАТНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ

А.М. Ковалев, чл.-корреспондент НАНУ,
В.А.Козловский, к.ф.-м.н., с.н.с.,
В.Ф. Щербак к.т.н., доцент,
Институт прикладной математики и механики НАНУ
e-mail: kozlovskii@iamm.ac.donetsk.ua

Одно из перспективных направлений в области современных коммуникационных технологий связано с использованием динамических систем, обладающих хаотическим поведением. На их основе, в частности, разрабатываются системы закрытия информации от несанкционированного доступа. Базовым свойством таких систем является обратимость. В терминах теории управления динамические системы, пригодные для преобразования и передачи информации, составляют класс обратимых систем управления. При этом многомерность динамической системы, наличие сложных взаимосвязей между переменными, позволяют конструировать системы разного уровня сложности. В работе обсуждаются вопросы построения различных типов обратных систем, как непрерывных, так и дискретных. Рассмотрены конструкции обратных систем, обладающих различной степенью обратимости: идентифицируемые, обратимые, обратимые на нескольких траекториях.

Динамическая система вход-выход

$$\dot{x} = f(x,u), \quad x(0) = x_0, \qquad y = h(x)$$

используется для передачи информации по следующей схеме: кодер (динамическая система) преобразует вход $u(t)$,

который является оцифрованным информационным сообщением, в траекторию системы дифференциальных уравнений (1). С помощью функции $h(x)$ траектория преобразуется в функцию времени (передаваемый сигнал) $y(t)$. Если соответствие между входом и выходом $u(t) \rightarrow y(t)$ является взаимнооднозначным, то существует возможность определения значений $y(t)$ по имеющейся информации об $y(t)$. В частности, если исходная система является обратимой, то для нее может быть построена обратная система, которая по сигналу $y(t)$ определяет исходное сообщение $u(t)$. Указан способ построения обратной системы. Ключом является совокупность начальных условий и некоторых параметров системы уравнений.

При реализации таких систем на компьютере, например, как криптографических систем, возникает необходимость перехода к дискретным аналогам непрерывных динамических систем. Такие аналоги предложены в виде конечных автоматов, описываемых системами уравнений над конечными полями или кольцами. При этом разные типы обратимости получают естественную теоретико-автоматную интерпретацию. Введено понятие k-кратного без потери информации автомата (к-БПИ), которое аналогично понятию обратимости на нескольких траекториях. Для ряда систем (Лоренца, Ресслера, Чуа) введены их автоматные аналоги и на их основе предложены поточные криптоалгоритмы. В рамках теории экспериментов с автоматами выполнена формализация атак на такие криптосистемы и доказана NP-полнота задачи о распознавании контрольного эксперимента для к-БПИ-автоматов, лежащая в основе такой формализации. Предложенные алгоритмы реализованы и приведены результаты их работы при передаче текстовых, графических и звуковых сообщений.

УДК 681.3.06 : 519.248.681

АПАРАТНА ІМПЛЕМЕНТАЦІЯ ПОМНОЖУВАЧІВ ДЛЯ КРИПТОГРАФІЇ ЕЛІПТИЧНИХ КРИВИХ

Л.М. Тимошенко, к.т.н., доцент,
e-mail: lmt0902@gmail.com
Ю.М. Чайківська, магістр
Тернопільський національний економічний університет,
e-mail: u_chaika@yahoo.com

Існує ряд задач, в яких поряд з програмною реалізацією операцій шифрування є необхідною апаратна реалізація. Досліджено, що криптографія еліптичних кривих (ЕКК) дозволяє при тій же довжині ключа, що й RSA, отримати більшу швидкодію і надійність.

Багато апаратних реалізацій операції множення для (ЕКК) не здатні конкурувати з існуючими програмними. Лише апаратна реалізація арифметики в скінчених полях симулює поодиноку роботу її модулів з використанням певних інструментів.

Всі модифікації алгоритму Монтгомері спрямовані на зменшення часу виконання схеми для практичної реалізації апаратного забезпечення, тобто збільшується продуктивність системи. Для проведення дослідження розглядалися швидкий та пришвидшений алгоритм Монтгомері.

Для порівняння різних алгоритмів нам потрібна модель складності, яка дозволяє реально оцінити вимоги до часу реалізації даних методів. Затримка повного суматора (одиниця часу) взята як посилання на вимоги часу виконання і визначає кількість затримок доступу до таблиці пошуку із такою ж затримкою одиниці часу. Ці

значення забезпечують реалістичну модель для оцінки часу виконання більшості алгоритмів модулярного множення.

Для проектування схеми на основі швидкого і пришвидшеного алгоритмів множення Монтгомері було використано мову опису інтегрованих компонентів апаратного забезпечення (VHDL). Для реалізації помножувачів було використано структурний підхід.

Мінімальний період часу і абсолютний час для кожної реалізації різний і зображений відповідно на рисунках 1 і 2. Абсолютний час виводиться з мінімального періоду часу наступним чином:

$$Абсолютний\ час = (Мінімальний\ період) * (число\ тактів),$$

$$число\ тактів = довжині\ бітів\ (n) + 1.$$

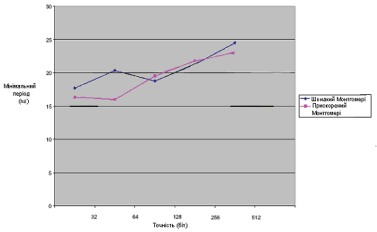


Рисунок 1. Мінімальний період часу всіх виконань

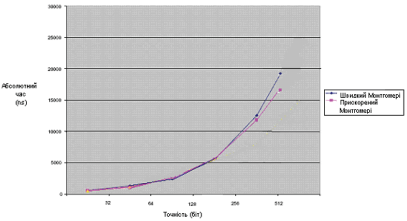


Рисунок 2. Абсолютний час даних реалізацій

Збільшення бітової послідовності шляхом піднесення до степеня 2 веде до приблизного збільшення абсолютного часу. В якості помножувача для ЕКК ефективніше використовувати пришвидшений алгоритм Монтгомері.

На далі плануємо реалізувати модифікацію алгоритму Монтгомері - модульне множення з чергуванням і дослідити його на ефективність апаратної імплементації.

УДК 681.3

ЗАХИСТ ДАНИХ В ІНФОРМАЦІЙНІЙ ТЕХНОЛОГІЇ НА ОСНОВІ ЦИФРОВИХ ПОШТОВИХ МАРОК

І. А. Дичка, д.т.н, професор, Д. В. Проскурін, аспірант
Національний технічний університет України
“Київський політехнічний інститут”
e-mail: dimacfc@gmail.com

Одним з перспективних напрямків розвитку галузі доставлення поштових відправлень є інформаційна технологія, що грунтується на застосуванні так званих цифрових поштових марок – технологія DPM (DPM – Digital Postage Mark). DPM – це спеціальне зображення, основним елементом якого є двовимірна дискретна графічна позначка, що є графічним (штриховим) кодом. Дані з DPM знімаються за допомогою сканування графічного коду з подальшою обробкою відсканованої інформації.

Головними перевагами використання DPM є висока щільність зберігання даних, придатність їх до машинного зчитування та обробки, можливість автентифікації поштових відправлень. Але використання відкритих електронних мереж зв’язку та потреба у високому рівні безпеки пересилання об’єктів висувають досить жорсткі вимоги до організації засобів захисту інформації.

Для цього при розробленні технології слід проводити комплексний аналіз можливих загроз та створити методику захисту від них.

Окремою, і досить важливою проблемою при доставці поштових відправлень є так звані підміни, тобто несанкціоновані дії третіх осіб, пов’язані з використанням дублікатів вже існуючих цифрових поштових марок. Тому

особлива увага має приділятися процедурі автентифікації кореспонденції, тобто визначенню унікальності кожного поштового відправлення. Цього можна досягти за рахунок застосування алгоритмів криптографічного захисту інформації і, зокрема, електронного цифрового підпису, затвердженого відповідним законодавством, зокрема Державними стандартами України. Криптографічні засоби захисту інформації мають застосовуватись не лише при пересиланні службової інформації через електронні мережі зв'язку, але й на етапі кодування даних при формуванні самої DPM. Тобто, фізичне нанесення службової інформації (у вигляді зображення DPM) на об'єкт або поштове відправлення виключає вплив загроз, характерних для передачі даних по незахищених електронних мережах.

При розробці технологічних засобів безпеки слід враховувати також надійність програмного забезпечення, яке надається користувачам для відправлення кореспонденції, а також брати до уваги відкритість електронних каналів зв'язку, які застосовуються для передачі службової інформації.

До організаційних аспектів безпеки можна віднести заходи з координування дій персоналу, проведення своєчасного контролю доставлення кореспонденції на різних етапах її фізичного транспортування, виявлення підмін та відповідні дії з реагування тощо.

В доповіді розглядається ряд вимог до рівня безпеки та захисту інформації, які висуваються при розробці технологій та проектуванні технічних засобів на основі використання DPM. Характер та ступінь вимог можуть підлягати певним змінам залежно від наявних потреб, враховуючи також особливості застосованих стандартів захисту інформації. Пропонуються можливі напрямки підвищення безпеки використання технологій на основі DPM.

УДК 621.363.6

БЕЗПЕКА ПЕРЕДАЧІ ПОВІДОМЛЕНЬ В БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

І.С. Литвин, к.т.н., доцент
Тернопільський національний
економічний університет
e-mail: lytvyn_igor@inbox.ru

Процес криптографічного шифрування даних в банківських системах захисту інформації можна здійснювати, як програмно, так і апаратно. Апаратна реалізація відрізняється істотно більшою вартістю, однак їй властиві і переваги: висока продуктивність, простота, захищеність. Безпека передачі повідомлень в сучасних банківських інформаційних системах основана на ключах, а не на деталях алгоритмів і тому багато алгоритмів шифрування відкриті і можуть бути проаналізовані, а програмні і апаратні засоби призначенні для їх реалізації можна купувати і продавати. В даній роботі проведено аналіз найбільш важливих характеристик алгоритмів шифрування повідомлень в банківських інформаційних системах: економічної ефективності (вартості) застосування алгоритму, криптографічної стійкості, швидкості виконання алгоритму на основних апаратних та програмних платформах.

Для забезпечення конфіденційного обміну інформацією між двома філіями одного банку процес обміну ключами може бути досить тривіальним, проте в банківській інформаційній системі, де кількість клієнтів складає десятки і сотні тисяч, управління ключами - серйозна проблема. Тому що вартість застосування

алгоритму, пов'язана з числом можливих з'єднань з клієнтами, що визначається за формулою $(n^2 — n)/2$, де n — число клієнтів серед яких необхідно поширювати секретних ключі у банківській мережі передачі даних.

У системі електронного банкінгу з одним мільйоном клієнтів можливо біля $5*10^{11}$ з'єднань, і вартість поширення ключів виявляється неприйнятно високою для банку.

Необхідність забезпечення криптографічної стійкості при передачі повідомлень в банківській інформаційній системі, призначеній для масового застосування, ставить високі вимоги до алгоритмів шифрування і до ключів.

Стандартний алгоритм шифрування повідомлень в розподіленій банківській інформаційній системі повинен забезпечувати можливість його реалізації в реальному масштабі часу на розподілених неоднорідних апаратно - програмних платформах, які, відповідно, пред'являють до нього різні вимоги.

Проведений аналіз досліджень нових методів захисту електронних повідомлень в банківських інформаційних системах дозволяє відмітити, що для найшвидшого виконання програм на яких написані алгоритми шифрування, завжди використовують спеціальні пристрої, однак програмні реалізації алгоритмів застосовують частіше.

УДК 681.324:007:681.3.068

ОСОБЛИВОСТІ РОБОТИ АВТОМАТИЧНИХ СИСТЕМ БОРОТЬБИ ЗІ СПАМОМ

О. М. Хошаба, к.т.н., доцент, С. В. Крилов, інженер
Вінницький національний технічний університет
e-mail: Alexander@Hoshaba.org, s_cr@vstu.vinnica.ua

В теперішній час актуальними питаннями залишаються зниження кількості непотрібних (рекламних) електронних поштових повідомлень що надсилається користувачам. Таке явище отримало назву спам. Як правило, у розвинутих країнах за це існує кримінальна відповідальність в зв'язку з тим, що суспільство щорічно втрачає великі кошти.

На сьогоднішній день існує безліч методів боротьби зі спамом. Всі вони мають різну ефективність роботи. До таких методів відносяться байєсові фільтри, сірі та білі списки. Технології розпізнавання непотрібних (рекламних) електронних повідомлень полягають у різній реакції спамерських серверів на запити поштових програм. Системи, що використовують такі та інші методи і відомі своєю ефективною роботою поділяються на автоматичні та автоматизовані. В значній мірі, вони мають свої переваги та недоліки. Однак вважається, що автоматичні системи, тобто програмно-технічні комплекси, робота яких здійснюється без участі людини є найбільш продуктивними та перспективними у боротьбі зі спамом. Оцінка ефективності їх роботи досягає 70-95%.

В роботі оглянуті переваги та недоліки таких систем і методів їх роботи. Визначені структурні особливості побудови автоматичних систем. Наведено ряд прикладів.

УДК 681.324:007:681.3.068

ОСОБЛИВОСТІ БЕЗПЕЧНОЇ РОБОТИ ДОМЕНИХ СИСТЕМ ІМЕН

О. М. Хошаба, к.т.н., доцент, В. Д. Ференець, інженер
Вінницький національний технічний університет
e-mail: Alexander@Hoshaba.org, frictory@vstu.vinnica.ua

Одною з самих важливих служб міжнародної комп'ютерною мережі Інтернет є система доменних імен (DNS). Практично всі інші служби міжнародної комп'ютерної мережі Інтернет майже завжди користуються послугами DNS. Доменна система імен виконує багато важливих функцій, однак однієї відомої зі всіх них є перетворення імен комп'ютерів у IP-адреса та навпаки. Тому доменна система імен представляє собою розподілену базу даних яка вирішує проблему найменування комп'ютерів що підключені корпоративних мереж Інтернет.

За свідоцтвом американських вчених, більш ніж 98% потоків даних що надходять до серверів імен (DNS сервери) вважаються зайвими. Також, до недавно ще успішно проводяться атаки на DNS сервери. Так, відомий напад на американський домен що зумів зупинити 8 з 13 потужних серверів. Тому, важливими є вивчення недоліків роботи та розробка сучасних механізмів ефективної та безпечної роботи DNS серверів.

Насамперед, це стосується розпізнавання потоків даних що надходять до DNS серверів та визначення об'єму апаратних ресурсів що споживають сервера імен.

В роботі показано особливості функціонування серверу імен. Визначено структура та особливості безпечної роботи доменних систем імен. Наведено ряд прикладів.

УДК 681.3.06

МЕТОД ВИЗНАЧЕННЯ ЗБИТКУ ІНФОРМАЦІЙНОЇ СИСТЕМИ, ЯКОГО ЗАПОБІГЛИ, ЗА УМОВИ НАЯВНОСТІ ІНФОРМАЦІЇ ПРО ЗАГРОЗИ

О.П. Дóренський, викладач
Кіровоградський юридичний інститут
Харківського національного університету
внутрішніх справ
e-mail: dorensky@ukr.net

На сьогоднішній день більшість систем забезпечення безпеки інформації (СЗБІ) не відповідають вимогам організації надійної безпеки інформаційної системи (ІС), що пов'язано з рядом факторів, які не враховано на етапі проектування СЗБІ, однією з яких є проблема оцінювання показника якості СЗБІ.

Припустимо, сукупність загроз, які можуть загрожувати ІС і надходять від джерела загроз, є кінечними та підлягають підрахунку $i = \overline{1, n}$. Кожна i-та загроза характеризується ймовірністю появи $P_{i\ загр}$ та збитком $\Delta q_i^{загр}$, який наноситься ІС. СЗБІ виконує функції повної або часткової компенсації загроз для ІС. Основною характеристикою СЗБІ є ймовірність усунення кожної i-ї загрози $P_{i\ загр}^{усун}$. Припустимо, що збиток W можна зменшити за допомогою загального збитку $\overline{W}$, якого запобігли, або збитку $\overline{\omega}_i$, якого запобігли, за рахунок ліквідації дії i-ї загрози. Необхідно вибрати варіант реалізації СЗБІ, яка забезпечує максимум запобігання збитку від дії загроз за допустимих затрат на СЗБІ, тобто знайти

$$T^0 = \arg \max \overline{W}(T), \quad T^0 \in T^+, \tag{1}$$

при обмеженні $C(T^0) \le C_{доп}$, (2)

де T – деякий вектор, який характеризує варіант технічної реалізації СЗБІ; T^+ – допустиме значення вектора T; T^0 – оптимальне значення вектора T; $C_{доп}$ – допустимі затрати.

Проведені дослідження показали, що

$$P^{усун}_{i\ загр} = \sum_{j=1}^{k} \alpha_{ij} \cdot x_{ij} + \sum_{j=k+1}^{m} \alpha_{ij} \cdot \mu(x_{ij}), \tag{3}$$

де $\alpha_{ij} = \dfrac{\partial P^{усун}_{i\ загр}}{\partial x_{ij}}$ – величина, яка характеризує ступінь впливу вимог на ймовірність усунення i-ї загрози, x_{ij} – ступінь виконання j-ї вимоги до СЗБІ для усунення i-ї загрози, $i = \overline{1,n}$; $j = \overline{1,m}$, $\mu(x_{ij})$ – функція приналежності до найкращого значення j-ї якісної вимоги і оцінка величини $\overline{W}$ уникнутого збитку приймає вигляд

$$\overline{W} = \sum_{j=1}^{n} \sum_{j=1}^{k} \overline{\lambda_i} \cdot \Delta q_i \cdot \alpha_{ij} \cdot \overline{x}_{ij} + \sum_{i=1}^{n} \sum_{j=k+1}^{m} \overline{\lambda_i} \cdot \Delta q_i \cdot \alpha_{ij} \cdot \mu(x_{ij}). \tag{4}$$

. Таким чином, задача синтеза СЗБІ у вигляді (1), (2) зводиться до оптимального обґрунтування кількісних та якісних вимог до СЗБІ за допустимих затрат на СЗБІ і набуває вигляду:

знайти $\max \overline{W}(x_{ij}; i = \overline{1,n}; j = \overline{1,m})$, (5)

при обмеженні $C(x_{ij}) \le C_{доп}$; $i = \overline{1,n}; j = \overline{1,m}$.

Отже, знайдено ефективний метод визначення показника збитку ІС, якого запобігли, за умови наявності інформації про загрози.

УДК 004.9: 338

ЗАСТОСУВАННЯ МЕТОДИКИ FTA У КОМП'ЮТЕРНОМУ УПРАВЛІННІ РИЗИКОМ НА ПРОМИСЛОВИХ ПІДПРИЄМСТВАХ

В. Кубіньські, професор, wkubinsk@zarz.agh.edu.pl
Е. Кубіньська–Калєта, асистент, ekaleta1@op.pl
Гірничо-металургійна академія (м. Краків, Польща)

Дерево непридатності FTA, як визначено в літературі, являє собою графічне представлення певних умов й інших компонентів, котрі викликають або приводять до появи визначеної *неочікуваної події*, котра має назву *„пікова"*. Методика FTA уможливлює розробку алгоритму, що моніторує ризик і дозволяє створити комп'ютерну програму управління й моніторингу усіх видів ризику. Аналіз систем з використанням *дерев непридатності* – дедуктивний метод (згори донизу) має на меті викриття причин або їх комбінацій, що можуть допровадити до визначеної *„пікової події"*.

Створення *дерева* розпочинається від визначення *пікової події*. Розбудова гілок *дерева* закінчується у той час, коли появляється одна або більше з перерахованих нижче *подій: головні,* тобто незалежні, для яких істотні характеристики можуть бути визначені в інший спосіб ніж за допомогою *дерева непридатності; події*, котрі не потребують розбудови у подальшому; *події*, котрі були або будуть розбудовані в іншому *дереві непридатності*. У прикладі, що аналізується, *„піковою подією"* є збільшення ризику, пов'язаного з безпекою праці. До *головних подій* належать: виготовлення машин й устаткування з дефектних деталей, дешевших та гіршої якості; неретельний контроль якості у виробника машин й

устаткування; приховані вади матеріалів, з яких виробляються машини й устаткування; ушкодження під час транспортування; нестача фінансових коштів на модернізацію; погано організоване навчання, що стосується обслуговування устаткування; відсутність перевірки знань, отриманих під час навчання; неретельний аналіз попиту на навчання даної посади; нестача фінансових коштів на навчання; застосування попередніх дій алгоритмів – суб'єктивно вигідніших або швидших; відсутність зацікавлення або залучення до навчання з боку працівників; навчання, що ведеться в малозацікавлений і активний спосіб; нестача фінансових коштів в момент необхідності проведення огляду; недостатня кількість осіб, що працюють у відділах контролю, дотримання норм безпеки праці; перевантаження, викликане значним часом праці; рутина в діях; поганий психофізичний стан працівника; відсутність доброї якості охоронного устаткування; необхідність праці зі шкідливими речовинами і в шкідливих для здоров'я умовах праці, обумовлених специфікою технології; терористичний акт; занедбання періодичних досліджень; тощо. Вони впливають на *посередницькі події.* В процесі управління ризиком необхідно ретельно досліджувати й запобігати *головним подіям,* щоб не допустити виникнення *посередницьких подій.* Однак, в момент повстання *головної події* необхідно обмежити дії її наслідків, що сприяють подальшому повстанню *неочікуваних* явищ, які у свою чергу впливають на *посередницькі події.* То є, так званий, ефект доміно. Негативні показники, які діють на *головні події*, спричиняють негативні ефекти *посередницьких подій.* Якщо ці показники не обмежити, то автоматично у напрямку в верх по гілках *дерева непридатності* буде обмежено ефекті *„пікової події".* Проте, необхідно пам'ятати, що деяким *головним подіям* неможливо протидіяти (наприклад, терористичний акт).

УДК 004.9: 338

СТВОРЕННЯ АЛГОРИТМУ УПРАВЛІННЯ РИЗИКОМ В ПРОМИСЛОВИХ ЗАКЛАДАХ

Е. Кубіньська-Калєта, асистент
e-mail: ekaleta1@op.pl
Р. Зубков, стипендіат програми Л. Кіркланда 2006/2007
e-mail: rzubkov@poczta.zarz.agh.edu.pl
Гірничо-металургійна академія (м. Краків, Польща)

Завдання алгоритму – виділення головних *подій,* що приводять до збільшення досліджуємого ризику, за допомоги *дерева непридатності FTA,* а також протидіяти їм, використовуючи утворений з тією метою *список рішень*. Після запуску алгоритму перевіряється чи ризик збільшився. Якщо *ні,* то алгоритм закінчує свою дію; якщо *так,* то задається величина *k,* котра вказує на кількість *подій* в *дереві непридатності*. Далі зостає урухомленою петля, котра при кожному своєму оберті перевіряє окремо усі *події.* Перша умовна інструкція перевіряє чи *подія,* котра є предметом дослідження, була раніше виключена з *подій,* котрі мають бути проаналізовані у подальшому. Якщо ця умова виконується, то перевірка цієї події у цьому місці закінчується й відбувається перевірка наступної або припинення дії петлі, що залежить від номеру перевіряємої події. У випадку якщо *подія* не була виключена раніше, то відбувається перехід до наступної умови, котра перевіряє чи дана *подія* виконується або зостала виконана. Якщо не виконується, то усі *події*, будучи подпричинами досліджуємої, стають виключеними з подальшого аналізу. Проте якщо *подія* виконується, то переходимо до остатньої умови, котра перевіряє чи *подія,* котра є предметом дослідження, є *головною*, а далі не розкладеною на

подпричини. Якщо *ні*, то завершується перевірка даної *події*, проте припускаючи, що *так*, повинні бути застосовані попереджувальні заходи, котрі торкаються цієї *події*. Так, по черзі перевіряються усі *події*, що розташовані у *дереві непридатності,* після чого настає вихід з петлі й закінчення дії алгоритму. Цей алгоритм є тісно пов'язаний з *деревом непридатності* і тільки у поєднанні з ним може ефективно функціонувати. Можливе, що проведення аналізу представленим алгоритмем не дозволить віднайти причини збільшення досліджуємого ризику. Належить тоді шукати причин проблеми поза алгоритмем. По знаходженню належить відповідно їх розместити в *дереві непридатності,* щоб у майбутньому було можливе аналізувати цю причину за допомгою алгоритму.

Для використання у повному обсязі можливостей алгоритму необхідно:

- визначити актуальні проблеми й ті, що можуть з'явитися у майбутньому, визначити для кожної з них за допомогою методики FTA або інної *головні події,* котрі викликають ці проблеми. *Дерево непридатності* актуалізувати у випадку зміни існуючої або появлення нових проблем, пов'язаних з ризиком, що досліджується,
- знайти можливі оптимальні вирішення, які можна застосувати, щоб запобігти неочікуваним *подіям*; обмежити їх або зліквідувати. Виконати це для кожної неочікуваної *головної події* з отриманих у попередньому пункті. Вирішення актуалізовувати кожного разу, коли є актуалізоване *дерево непридатності* та у випадку зміни існуючих або появлення нових ідей вирішення,
- урухомити алгоритм й слідувати інструкції; використовувати регулярно згідно визначених індивідуальне вказівок або в моменті збільшення даного ризику.

УДК 004.056

БАГАТОВИМІРНІ МАТРИЦІ ДОСТУПУ ЯК ЗАСІБ РЕАЛІЗАЦІЇ ПОЛІТИКИ БЕЗПЕКИ В СУЧАСНИХ АВТОМАТИЗОВАНИХ СИСТЕМАХ

К.О. Липинець, магістрантка,
О.С. Михайлюк, н.с., В.Е. Тамберг, н.с.
Національний технічний університет України
“Київський політехнічний інститут”
e-mail: may@scs.ntu-kpi.kiev.ua

Розширення спектру форм застосування автоматизованих систем в практично усіх сферах людської діяльності призводить до підвищення вимог щодо гнучкості підсистеми захисту комп’ютерної інформації. Це в свою чергу вимагає удосконалення способів формалізованого відображення та засобів реалізації політик безпеки інформації. Так, зокрема, квазістатичні форми подання функціональності захищених систем на зразок традиційних матриць доступу часто є не досить мобільними в контексті сучасних комп’ютерних систем з витонченими механізмами керування безпекою.

У доповіді пропонується концепція удосконаленої багатовимірної матриці доступу. Її застосування полегшує врахування наявних у політиці безпеки залежностей між режимами доступу та такими важливими параметрами як зокрема дислокація користувача (IP-адреса комп’ютера, з якого надходить запит на доступ), системний час, передісторія (наприклад, часткова або повна дискредитація суб’єкта тощо). Запропоновано машинно-орієнтовані форми подання багатовимірних матриць доступу у вигляді полікубів та гіперкубів. Наводяться перевірені у ході дослідного впровадження алгоритми керування доступом.

УДК 681.3

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМ КЕРУВАННЯ ДОСТУПОМ ІЗ ЗАСТОСУВАННЯМ БЕЗКОНТАКТНИХ ІДЕНТИФІКАТОРІВ

Л.Г.Сердюк, н.с., О.О.Лещенко, м.н.с.,
Є.В.Шпак, магістрант
Національний технічний університет України
“Київський політехнічний інститут”
e-mail: may@scs.ntu-kpi.kiev.ua

Сьогодні широко розповсюдженим засобом введення ідентифікаційних ознак у ході аутентифікації користувача автоматизованої системи є так звані безконтактні ідентифікатори у формі магнітних карток, жетонів, брелоків тощо. Однак традиційний спосіб застосування безконтактних ідентифікаторів лише для отримання дозволу на доступ до захищеного ресурсу далеко не вичерпує їх дійсний потенціал. Зокрема, можливість дистанційного зчитування вмісту ідентифікаторів дозволяє здійснювати фоновий моніторинг присутності користувачів та персоналу навколо відповідних контрольних точок як у безпосередній близькості від автоматизованої системи, так, загалом, і у межах деякого периметру.

Пропонується інтелектуалізований програмно-апаратний комплекс безперервного багатопараметричного контролю дотримання умов доступу до ресурсів автоматизованої системи. Апаратна компонента комплексу являє собою сукупність розташованих у межах контрольованого простору і узгоджених за радіусом дії зчитувачів RFID-ідентифікаторів - магнітних карток класу «Ангстрем» та «EM-Marin». Отримана у результаті

моніторингу модель просторового розташування суб'єктів доступу, наприклад користувачів, персоналу, активних ресурсів автоматизованої системи, сторонніх ресурсів тощо, порівнюється з так званою технологічною картою захищеного ресурсу, доступ до котрого ініціюється або здійснюється. Індивідуальна технологічна карта захищеного ресурсу являє собою формалізоване подання відповідних розділів політики безпеки. Зокрема вона містить ієрархію варіантів просторового розташування суб'єктів доступу. У згаданій ієрархії виділено варіанти, технологічно необхідні, дозволені та заборонені у контексті ініціювання та власне здійснення доступу. Таким чином, співставлення результатів моніторингу контрольованої зони з технологічною картою дозволяє ідентифікувати ситуацію, на основі чого автоматично приймається рішення щодо дозволу чи заборони доступу як при його ініціюванні, так і у ході реалізації.

У доповіді докладно розглядається алгоритмічна організація програмної компоненти комплексу. Її ядром є експертна система реального часу, призначена для підтримки прийняття рішень щодо управління доступом. Механізм виведення експертної системи базується зокрема на математичному апараті нечіткої логіки. В експертній системі реалізовані засоби навчання, завдяки чому у ході її експлуатації формуються і уточнюються моделі суб'єктів доступу. Наявність моделей дозволяє здійснювати додаткову оцінку критичності подій та процесів і у разі необхідності вживати превентивних заходів щодо управління доступом

В доповіді наводяться результати дослідження ефективності запропонованого підходу до управління доступом. Показано, що найбільший ефект отримується при його застосування для захисту розподілених автоматизованих систем.

УДК 004.056

ПРОБЛЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПОШУКОВИХ ІНТЕЛЕКТУАЛЬНИХ АГЕНТІВ

Т.Г. Сапсай, к.т.н., доцент,
Т.М. Заболотня, аспірантка, С.О. Єзжельонок
Національний технічний університет України
“Київський політехнічний інститут”
e-mail: may@scs.ntu-kpi.kiev.ua

Підвищення вимог щодо швидкодії, обсягу охопленого ресурсу та релевантності пошуку стимулює широке впровадження до сучасних мережевих інформаційно-пошукових систем найновіших ефективних програмних технологій, до числа котрих можна віднести технологію інтелектуальних програмних агентів. Однак, реалізація критичних з огляду на кінцевий результат елементів пошуковиків у вигляді автономних агентів додатково загострює проблему їх безпеки.

У доповіді аналізується проблема захисту інформації, котра обробляється пошуковими інтелектуальними програмними агентами, що функціонують у автономному режимі. Досліджується специфічний для пошукових агентів комплекс загроз щодо несанкціонованого доступу до інформації. З огляду на притаманну автономним агентам здатність до суспільної поведінки, про-активність, наявність ментальних властивостей тощо пропонується концепція корпоративної політики безпеки утвореного пошуковими агентами середовища самостійних програмних одиниць, а також концепція корпоративного комплексу засобів захисту. Розглядаються особливості забезпечення безпеки реактивних агентів, а також агентів, здатних до самостійного утворення та узгодження мети.

УДК 004.9

РОЗШИРЕННЯ ФУНКЦІОНАЛЬНОСТІ ПРОГРАМНИХ СИСТЕМ З ДОПОМОГОЮ АСПЕКТНО-ОРІЄНТОВАНИХ БІБЛІОТЕК

А.І. Олефіренко, аспірант
НаУКМА,
e-mail: andriyo@gmail.com

Метою роботи є дослідження ефективності використання аспектно-орієнтованих бібліотек для розробки складних програмних систем. Дослідження робиться на основі розробленої нами бібліотеки класів та аспектів, яка використовувалась для створення автоматизованої системи керування вищим навчальним закладом. Однією з найбільш потужних компонент бібліотеки є набір класів та аспектів, призначених для декларативного керування правами доступу до довільних елементів програмної системи.

Бібліотека розроблювалась з метою використання багатьма розробниками, в тому числі і тими, хто ще не достатньо володіє технікою написання безпечного коду. Під безпечним кодом вважаємо такий функціонально правильний код, який максимально обмежує неправильне використання його чи то на рівні інтерфейсу з користувачами, чи то іншими програмістами. Тобто йдеться про помилки в написанні коду, які уможливлюють непередбачену специфікаціями функціональність. Причина таких помилок полягає в тому, що під час проектування розробники зазвичай приділяють мало уваги таким сторонам системи як перевірка вхідних параметрів, перевірка прав доступу на той чи інший об’єкт чи його

метод тощо. Зазвичай програмісти в останню чергу дороблюють вже існуючу систему з урахуванням цих додаткових аспектів.

Аспектно-орієнтована бібліотека, створена нами для вирішення подібного класу проблем, дозволяє у декларативному вигляді (у вигляді аспектів) примусово до вже існуючого коду внести додаткову функціональність, яка і буде реалізовувати всі необхідні дії щодо перевірки прав доступу, правильності викликів методів, використання класів тощо, тобто ті дії, які необхідні для безпечного коду. Зауважимо, що бібліотека максимально прозора для використання: програміст може зосередитись на написанні предметнозалежного коду, а потів вже додати до нього предметнонезалежну функціональність, якою по суті є безпечність коду. Так само можуть бути додані інші предметно-незалежні функціональності: журналювання, керування трансакціями тощо.

Дослідження може бути використане для прийняття рішення щодо доцільності використання аспектно-орієнтованих бібліотек на зразок розробленої нами. Очевидно, що розділення функціональності системи на предметну та предметнонезалежну дає можливість повторного використання предметнонезалежної частини. Повторне використання збільшить надійність коду та швидкість створення програмних систем в цілому. В той же час, не завжди вдається проводити дизайн та розробку системи в такому виглядів, щоб вона ідеально підходила для використання з аспектно-орієнтованими бібліотеками. В будь-якому разі, наявність в інструментарії архітекторів та розробників аспектно-орієнтованих бібліотек дає їм ще один інструмент для створення високоякісних інформаційних систем.

UDC 681.3

DECISION SUPPORT SYSTEM ON TELECOMMUNICATIONS SECURITY INCIDENTS RESPONSE AND HANDLING

S.V. Gladysh,
Master of Telecommunications, post-graduate
Odessa national academy of telecommunications
e-mail: sglad@i.ua

The consequence of telecommunications technology development trends is necessity to revise the traditional view of the security problem and to search for new adequate approaches to its solution. One of such approaches, which consider these trends, is ***artificial intelligence*** and ***decision support systems*** *(DSS).*

Development of intellectual systems aimed to telecommunications security remains to be actual scientific problem. ***Telecommunications security incidents response and handling*** is one of the most important parts of this problem. There are international standards (*ISO 27001:2005; ISO 17799:2005*) and recommendations (*ITU-T E.409; RFC 2350, BCP 21*) where the terms "security incident", "information security incident", "incident response" etc. are defined. But analysis of the latest publications, the given standards and recommendations shows: there is neither rather effective practical nor completely adequate theoretical model for development of DSS on telecommunication security incidents response and handling.

The purpose of the research is to develop such a model, by integration of knowledge representation languages, adequate to the specificity of telecommunications security incidents

response and handling, and thus convenient for the methodology of DSS development.

In the most common definition, the task can be reduced to development of a model, which would allow forming a selection function of an optimal strategies subset at the choice of incident response or handling decision variant.

Recommendation ITU-T E.409 and PDCA model are used as the base for telecommunications security incidents management procedures and life cycles description. Interconnections and the place of the developed decision support system in these procedures are showed on figure 1.

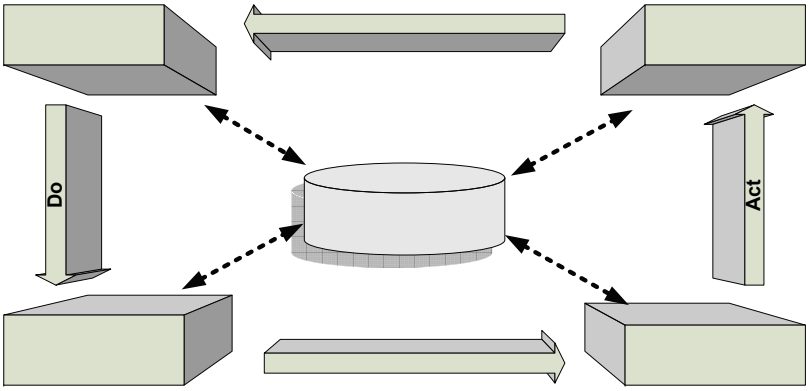


Figure 1 – Functional scheme of decision support system

DSS is presented by 3 interconnected models: an object model, a dynamic model and a functional model. Knowledge representation model is synthesized by integration of Jang adaptive fuzzy neural network ANFIS (Matlab) and Colored Petri net (CPN tools):

$$KRM = ANFIS \cup CPN \qquad (1)$$

The result of the given research is a methodological approach to synthesis of DSS with hybrid network knowledge representation model of telecommunications security incidents response and handling.

УДК 681.3.06

АНАЛІЗ РЕЗУЛЬТАТІВ РОБОТИ НЕРЕКУРЕНТНОГО ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

А.С. Васюра, к.т.н., професор,
С.В. Юкиш, аспірант
Вінницький національний технічний університет
e-mail: Yukish@svitonline.com

Генератори псевдовипадкових послідовностей (ГПВП) є важливою складовою криптографічних алгоритмів та протоколів. Якість таких протоколів та алгоритмів значною мірою залежить від швидкодії та якості використаних ГПВП. Якісний ГПВП повинен створювати послідовність, яка за характеристиками наближається до випадкової послідовності. На практиці, для доказу того, що ГПВП створює якісну послідовність чисел, використовується статистичне тестування послідовностей.

Відомі на сьогодні ГПВП, так чи інакше засновані на принципі рекурсії, тобто кожний елемент послідовності залежить від попередніх значень послідовності, або внутрішніх станів генератора. Не існує простої формули визначення за номером позиції та ключем чергового елементу послідовності. На кожному такті шифрування над матеріалом ключа та внутрішніми змінними потокового шифру виконуються певні однотипні перетворення, а через це кожен елемент фактично залежить від його положення в загальному потоці гами. Так, для того щоб отримати значення елементу n, необхідно визначити всі попередні $n-1$ елементів.

Нерекурентний ГПВП дає змогу уникнути цього недоліку. Це досягається тим, що такий ГПВП дозволяє визначити черговий елемент послідовності лише за номером позиції елемента та ключем. При використанні нерекурентного ГПВП виникає можливість економити не лише час, а й апаратні ресури в процесі шифруавння і дешифрування.

В даній роботі описується робота розробленого нерекурентного ГПВП. Принцип дії запропонованого ГПВП оснований на дискретизації математичної функції і виконанні перетворення над результатом, збереженим у числі з плаваючою точкою відповідно до стандарту IEEE-754.

Для поглибленого визначення характеристик послідовностей, створених ГПВП, й знаходження слабких місць у них, широко застосовується набір тестів NIST Statical Test Suite. Цей набір був спеціально розроблений для таких цілей Американським національним інститутом стандартів та технологій. NIST STS складається з 16-ти різноманітних тестів кожний з яких направлений на виявлення окремого типу “невипадковості” у послідовностях.

Послідовності створені запропонованим ГПВП проходять усі тести з вказаного набору й мають статистичні характеристики, що знаходяться в допустимих межах. На підставі цього можна вважати розроблений генератор таким, що створює статистично якісні послідовності.

УДК 681.32

БЛОКОВИЙ ШИФР НА ОСНОВІ АРИФМЕТИЧНИХ ОПЕРАЦІЙ ЗА МОДУЛЕМ

А. В. Лужецький, д.т.н., професор,
О.В. Дмитришин, студент
Вінницький національний технічний університет

Відомі блокові шифри реалізуються на основі сукупності арифметичних і логічних операцій та зсувів кодів. Однак найефективніше сучасні мікропроцесори реалізують арифметичні операції. Тому розробники перспективних блокових шифрів намагаються використовувати саме арифметичні операції за модулем 2^m для шифрування інформації. В доповіді розглядається побудова блокового шифру на основі арифметичних операцій за довільним модулем, який є секретним і є частиною ключів за шифрування і розшифрування.

Нехай X_0 – n-розрядний блок, тоді його зашифрування відбувається шляхом обчислень за формулою:

$$X = X_0 A \bmod m, \qquad НСД(A, m) = 1, \qquad (1)$$

а розшифрування блоку X за формулою:

$$X_0 = XA^{-1} \bmod m. \qquad (2)$$

При цьому ключ для зашифрування є конкатенацією $K=A||m$, а ключ розшифрування – $K=A^{-1}||m$.

Для забезпечення потрібної стійкості такого блокового шифру пропонується процедуру зашифрування (1) виконувати L разів ($L = \overline{2 \div (m-2)}$). Схематично процес зашифрування і розшифрування показано на рис. 1.

Якщо розрядність інформаційного блоку n_x, то розрядність коефіцієнта A доцільно обирати такою ж самою $n_x=n_A=n$, тоді розрядність модуля m має

дорівнювати $n_m=n+1$, тобто в деяких випадках зашифроване повідомлення може мати на один розряд більше порівняно з початковим блоком.

Інший підхід до побудови блокового шифру полягає в тому, що замість виконання L раундів обчислень з однаковими значеннями A і m пропонується здійснювати L раундів обчислень, в кожному з яких використовується інше значення m і A. При цьому має виконуватись умова $m_1<m_2<\ldots<m_L$. У даному випадку для кожного раунду використовується свій окремий секретний ключ $K_i = A_i||m_i$, $i = \overline{1 \div L}$. Схематично процес зашифрування і розшифрування показано на рис. 2.

Можливі варіанти формування K:

1. Якщо A_i =const, m_i = var, то $K=A||m_1||m_2||\ldots||m_L$.
2. Якщо A_i = var, m_i = const, то $K=A_1||A_2||\ldots||A_L||m$.
3. Якщо A_i = var, m_i = var, то $K=A_1||A_2||\ldots||A_L||$ $||m_1||m_2||\ldots||m_L$.

Зашифрування і розшифрування вимагає виконання L операцій множення за модулем, що значно менше порівняно з кількістю операцій, що потрібно для реалізації будь-якого відомого блокового шифру.

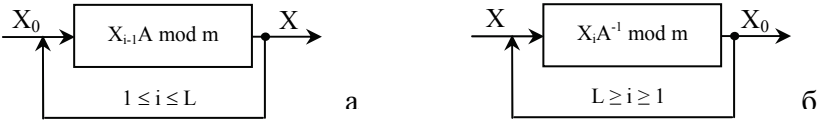


Рисунок 1 – Зашифрування A=const, m=const (а), розшифрування (б)

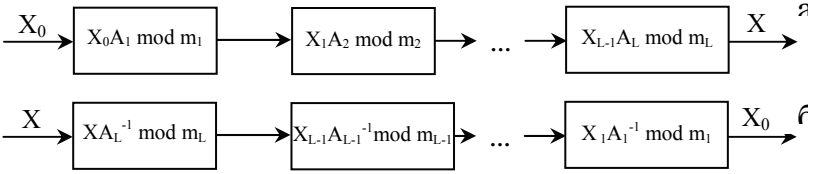


Рисунок 2 – Зашифрування A=var, m=var (а), розшифрування (б)

УДК 681.32

ПОТОЧНЕ ШИФРУВАННЯ НА ОСНОВІ ТЕОРІЇ ЛПМ

В. П. Семеренко, к.т.н., доцент,
Ю.В. Степанишин, студент, М.Л. Гаєвський, студент
Вінницький національний технічний університет
e-mail: sm@vinnitca.com

Базовими схемами при поточному шифруванні традиційно служать зсувні регістри із дуже простими функціями оберненого зв'язку. Такі схеми дуже уразливі до кореляційних атак, які дозволяють на основі послідовності невеликої довжини відкритого тексту відтворити структуру генератора псевдовипадкової послідовності. Для підвищення криптостійкості схем поточного шифрування використовують різноманітні схеми об'єднання зсувних регістрів (як, наприклад, у методі A5), або пропонується нелінійний обернений зв'язок.

Великі перспективи в розв'язанні проблеми підвищення криптостійкості схем поточного шифрування надає використання в криптоаналізі теорії лінійної послідовнісної машини (ЛПМ). В загальному випадку ЛПМ є автоматом лінійного типу, який над полем Галуа $GF(q)$ має функцію станів (переходів)

$$S(t+1) = A \times S(t) + B \times U(t)$$

та функцію виходів

$$Y(t) = C \times S(t) + D \times U(t),$$

де $U(t), Y(t), S(t)$ – вхідний вектор, вихідний, вектор і вектор станів; A, B – характеристичні матриці.

Матриця A визначає структуру обернених зв'язків

автомата, причому елементи останнього стовпчика або останнього рядка матриці A представляють собою коефіцієнти породжувального багаточлена

$$P(x) = p_0 + p_1 x + p_2 x^2 + \cdots + p_{r-2} x^{r-2} + p_{r-1} x^{r-1}, \quad GF(q)$$

Матриці B, C і D визначають відповідно структуру входів, структуру виходів відносно елементів пам'яті та структуру виходів відносно входів.

Традиційний регістр із оберненими зв'язками є двохполюсною ЛПМ, тобто ЛПМ з одним входом та одним виходом.

Пропонується використання багатополюсної ЛПМ, яка має f входів, f виходів і визначається такими характеристичними матрицями

$$A_{(f)} = \left| A^f \right|; \qquad B_{(f)} = \left| A^{f-1}B, \ldots, AB, B \right|;$$

$$C_{(f)} = \begin{vmatrix} C \\ CA \\ CA^2 \\ \cdots \\ CA^{f-1} \end{vmatrix}; D_{(f)} = \begin{vmatrix} D & & & & \\ CB & D & & & \\ CAB & CB & D & & \\ \cdots & \cdots & \cdots & \cdots & \\ CA^{f-2}B & CA^{f-3}B & \cdots & CB & D \end{vmatrix}.$$

Багатополюсна ЛПМ дозволяє генерувати псевдовипадкові послідовності максимальної довжини при різних комбінаціях вхідних сигналів. Це дає можливість переходу між різними циклічними послідовностями по заданим правилам. В результаті зменшується можливість відтворення структури генератора псевдовипадкової послідовності та збільшується в f разів швидкість шифрування.

Проведено дослідження криптостійкості багатополюсної ЛПМ по її аналітичній та графічній моделях.

УДК 681.3.067

ЗАСОБИ ОЦІНЮВАННЯ ЕЛЕКТРОМАГНІТНОЇ ОБСТАНОВКИ НА ВИДІЛЕНИХ ОБ'ЄКТАХ

Ю.П. Гульчак, к.т.н., доцент,
Вінницький національний технічний університет
e-mail: jurigulchak@rambler.ru
В.М. Дідич, аспірант
Вінницький національний медичний університет

Контроль електромагнітної обстановки в межах режимного об'єкта в режимі реального часу є актуальною проблемою, так як дозволяє оперативно фіксувати та аналізувати канали підозрілих електромагнітних випромінювань. На даний період застосовується велика кількість програмно-апаратних комплексів для виявлення і визначення рівня побічних електромагнітних випромінювань (ПЕМВ). Існуючі методи відрізняються засобами і способами фіксування рівнів ПЕМВ та аналізу електромагнітної обстановки, але всі вони потребують значних затрат часу. На практиці часто необхідно оперативно встановити розподіл електромагнітних полів у просторі і зміну їх з часом.

Для вирішення поставленої задачі запропонована система з сіткою локалізованих детекторів електромагнітного випромінювання, розміщених в окремих точках приміщення і сполучених через спеціалізований контролер з ПЕОМ. В якості первинних даних для аналізу використовується інформація отримана з здавачів рівня електромагнітного поля, а також бібліотека характерних випромінювань використовуваних у приміщенні пристроїв обчислювальної техніки, бібліотека характерних ознак

закладних пристроїв, отриманий заздалегідь статичний розподіл електромагнітного поля на виділеному об’єкті та база даних, яка фіксує зміну рівня випромінювання в конкретній зоні.

Результатом роботи системи є отримання динамічної карти електромагнітної обстановки на режимному об’єкті, яка в поєднанні з базою даних гранично допустимих значень і створеною стаціонарною картою для даного конкретного приміщення дає змогу чітко контролювати відхилення ПЕМВ з часом. Аналізуючи електромагнітне випромінювання в динаміці система відслідковує відхилення контрольованих параметрів не лише в конкретних точках простору, але і в межах всієї контрольованої зони. Система дозволяє оперативно змінювати місцезнаходження первинних індикаторів поля, змінювати їх кількість, але дана процедура вимагає відповідної зміни програмного забезпечення і створення оновленої стаціонарної карти електромагнітної обстановки.

Основним завданням моніторингу електромагнітної обстановки є виявлення і локалізація підозрілих джерел випромінювання, які будь-яким чином спотворюють карту стаціонарного розподілу поля. Важливим результатом роботи системи є ідентифікація нового джерела електромагнітного випромінювання на основі наявних бібліотек і трактування його як потенційно небезпечного. Програмне забезпечення системи дозволяє зберігати і протоколувати зміну електромагнітної обстановки протягом тривалого часу за періоди, задані відповідними службами організації.

Подальший аналіз виконується за допомогою спеціалізованих пошукових комплексів типу «Піранья» тощо.

УДК 681.3:621.396

ПРОЕКТУВАННЯ СИСТЕМ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВА

А.В. Дудатьев, к.т.н., доцент,
О.П. Войтович, к.т.н., ст. викладач
Вінницький національний технічний університет
e-mail: andreysaf60@mail.ru

Інформаційна система підприємства, як правило, складається з декількох рівнів управління, які в тій чи іншій мірі пов'язані між собою. Тому у зловмисників завжди знайдеться певний набір методів і засобів, які дозволять обійти політику безпеки підприємства, якщо він проник хоча б на один з них. Офіційна статистика представляє факти, які говорять про те, що більшість несанкціонованих спроб доступу до інформаційних ресурсів залишаються навіть невиявленими. Наприклад, за даними Національного відділення ФБР кількість невиявлених атак знаходиться в межах від 85% до 97%.

Звичайно, не всі недоліки, що привели до результативних несанкціонованих доступів до інформаційних ресурсів, в тому числі, і до найбільш захищених у світі, відомі. Тому постійно актуальним є питання проектування і оцінювання ефективності систем інформаційного захисту, які максимально ефективно реалізують відповідну політику безпеки.

Стандарт ISO/IEC 15408 визначає профіль системи захисту як сукупність функціональних і гарантійних вимог, які дозволяють реалізувати систему захисту з необхідним рівнем інформаційної безпеки. Методологія оцінювання

інформаційної безпеки профілю захисту базується на використанні методів аналізу і ідентифікації множини факторів, зокрема активи підприємства, недоліки в захисті, загрози, потенційні атаки тощо.

Необхідно зазначити, що відсутня чітка статистична інформація відносно об'єкта, який оцінюється і навпаки більшість процесів характеризуються невизначеністю. Все це робить неможливим практичне використання точних моделей, які базуються на класичній математичній теорії. Щоб вирішити ці проблеми, зручно використовувати апарат нечіткої логіки, де залежність входів системи та виходів задаються на основі лінгвістичної людської логіки, а не точних цифр, з якими складно працювати. Показники таких систем набагато вищі, ніж систем на чітких числах. Застосування конкретної діагностичної моделі залежить від виду порушення нормального ходу, вхідної інформації, знань експерта. У зв'язку з цим для отримання кількісної оцінки, що характеризує ефективність варіанта профілю захисту, пропонується використовувати експертні оцінки, що представляються у вигляді нечітких множин. Вибір значень елементів множини завжди пов'язаний з ризиком того, що обрані значення показників не забезпечують необхідного рівня безпеки. Наслідком цього є можливість провести ефективну атаку на відповідні інформаційні ресурси. Пошук наочного представлення знань приводить до систем на основі нечіткої логіки, яка забезпечує представлення словесно інтерпретованих знань.

Для забезпечення можливості прийняття рішення при не тільки кількісних, але й якісних характеристик, запропоновано використання нечіткого ієрархічного дерева, на основі якого будується база знань системи безпеки. Такий комплексний підхід надає можливість отримати на етапі проектування оптимальний варіант системи інформаційної безпеки підприємства.

УДК 681.3.06

АДАПТИВНИЙ МЕТОД ОЦІНЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ НЕВИЗНАЧЕНОСТІ

А.В. Дудатьев, к.т.н., доцент,
Ю.В. Баришев, студент
Вінницький національний технічний університет
e-mail: andreysaf60@mail.ru

Оцінка інформаційної безпеки є надзвичайно актуальною і складною, в той же час, задачею, оскільки її розв'язок потребує значних ресурсів. Але рішення задачі оцінки інформаційної безпеки і прийняття відповідних рішень щодо її захисту, як правило, виправдовує всі витрати. Знаходження відповідей на дані питання можливо отримати за допомогою математичного моделювання.

У відомих програмних продуктах @RISK, ALRAM, BDSS, LRAM для оцінювання ризику використовують традиційні кількісні методи. Засоби аналізу ризику BUDDY SYSTEM, CONTROL-IT, CRAMM, базуються на якісному підході і ймовірні втрати виражаються у лінгвістичній формі, наприклад, «ризик відсутній», «ризик середній» і т.п. Ці засоби вимірюють можливі втрати на базі метода послідовних наближень, метода дерева подій, метода нечіткої логіки. Проте вони не дозволяють враховувати фактор часу.

Для розв'язку задачі пропонується використовувати побудову нейро-нечіткої мережі, яка визначає оцінку захищеності об'єкту на основі нечітких експертних оцінок факторів, які впливають на ту, чи іншу складову безпеки, в тому числі й на інформаційну безпеку. Для опису оцінки

даних факторів пропонується використовувати функції належності у вигляді трикутників.

Оскільки пропонується враховувати всі фактори, які впливають на безпеку об'єкта, то пропонується ваги персептронів вхідного шару нейромережі змінювати в діапазоні всіх дійсних чисел, тобто, чим більше модуль ваги персептрона, тим більше значення даний фактор має на складову захищеності. Від'ємними коефіцієнтами будуть позначатися протидії загрозам, а додатними – загрози.

Наступні шари нейромережі будуть мати тільки додатні значення, оскільки виходи вхідного шару нейромережі можуть бути як додатними, так і від'ємними.

Оптимальною системою захисту авторами пропонується визначати ту, значення виходу нейромережі якої прямує до нуля зліва.

Важливою характеристикою нейромережі є її здатність навчатися, що дозволяє їй адекватно оцінювати захищеність об'єкту, за умови коректної оцінки факторів. Крім того, якщо на окремий тип захисту певний фактор почне впливати, то його вага зміниться і стане відмінною від нуля. Тобто даний метод дозволить враховувати вплив нових загроз або появу нових методів протидії ним.

Отже нейро-нечіткий підхід до оцінювання інформаційної безпеки враховує фактор часу, пристосовується до зміни характеру впливу факторів, дія яких буває як негативна, так і позитивна з точки зору захищеності об'єкту. Нейро-нечіткий метод оцінювання захисту інформації є ефективнішим за існуючі методи, оскільки зберігаючи їх позитивні сторони – можливість оцінити захист інформації за відсутності чітких вхідних даних, дозволяє без побудови нової математичної моделі врахувати дію нових факторів впливу на стан загальної захищеності об'єкту.

УДК 681.3.06

ОСОБЛИВОСТІ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ БСШ НА ОСНОВІ АРИФМЕТИЧНИХ ОПЕРАЦІЙ ЗА МОДУЛЕМ 2^n НА ПЛАТФОРМІ x86-64

В.В. Сокирук, аспірант
Вінницький національний технічний університет

Платформа x86-64 була запропонована компанією AMD як варіант еволюційного переходу до 64-розрядних обчислень шляхом модернізації платформи x86, що дозволяє використовувати існуюче програмне забезпечення одночасно з усіма можливостями та перевагами нової архітектури. Набір інструкцій x86-64 містить всі основні x86 інструкції, а також додаткові інструкції для виконання 64-розрядних арифметичних та логічних операцій. Першим процесором для платформи x86-64 став AMD Athlon64, а згодом аналогічний набір команд під назвою EM64T з'явився в процесорах фірми Intel.

Використання 64-х розрядних обчислень дозволяє досягти суттєвого збільшення продуктивності в задачах криптографічного захисту інформації, пов'язаних із виконанням обчислень над великими цілими числами (криптосистема RSA, деякі блокові шифри тощо).

Блоковий симетричний шифр (БСШ) на основі арифметичних операцій за модулем, запропонований в попередніх роботах автора, оперує n-розрядними цілими числами, де n – розмір блоку даних. Найбільш складною операцію даного БСШ є множення двох n-розрядних цілих чисел за модулем 2^n. Для її реалізації використовується алгоритм множення у стовпчик, в якому n-розрядне ціле

число розбивається на w-розрядні блоки, де w – розрядність процесора. Так, при n=128 та w=32 необхідно виконати близько 10 операцій множень та 14 додавань 32-розрядних цілих чисел (без урахування операцій запису/читання з пам'яті). У випадку використання 64-х розрядних операцій множення і додавання для обчислення результату операції множення двох n-розрядних цілих чисел за модулем 2^n при n=128 та w=64 достатньо виконати 3 операції множення та 2 додавання. В табл. 1 наведено продуктивність програмної реалізації даного БСШ мовою Ansi C на процесорі AMD Athlon64 в 64-х та 32-х розрядному режимах роботи.

Таблиця 1

Продуктивність програмної реалізації БСШ

Операція, що виконується	Кількість тактів	
	x86	X86-64
Зашифрування	246	98
Розшифрування	248	98
Розгортання ключа для зашифрування (розшифрування)	737 (1243)	302 (403)

Таким чином, використання 64-х розрядних обчислень дозволяє значно підвищити продуктивність БСШ на основі арифметичних операцій за модулем 2^n за рахунок суттєвого спрощення реалізації операцій множення n-розрядних цілих чисел та знаходження мультиплікативної інверсії за модулем 2^n.

Найбільш повільною залишається операція дзеркальної перестановки розрядів n-розрядного цілого числа, яка потребує для виконання більше 70 тактів процесора AMD Athlon64, оскільки її реалізація мовою C є складною і неефективною. Використання команд асемблеру та особливостей того чи іншого компілятору для реалізації даної операції може ще більше покращити продуктивність даного БСШ в цілому.

3. Методи та засоби ущільнення інформації

УДК 004.22+004.627+004.056.55

МЕТОД СЖАТИЯ И ЗАЩИТЫ ДАННЫХ НА ОСНОВЕ СЛОВАРНОГО КОДИРОВАНИЯ

И.В. Кудрявченко, к.т.н., доцент
Севастопольский национальный технический университет, e-mail: inform_kaf@mail.ru

Словарное кодирование, для которого символами первичного алфавита являются слова, а не буквы, является одним из вариантов равномерного блочного кодирования, если длина блока равна длине адреса ячейки словаря. В рассматриваемом методе применяется программный генератор случайных чисел для равномерного перемешивания словаря. Поэтому наряду со сжатием, возможность которого обосновывается теоремой кодирования для каналов связи (КС) без шумов, метод дополнительно обеспечивает защиту данных.

Работу кодера источника (КИ) поясняет рисунок 1.

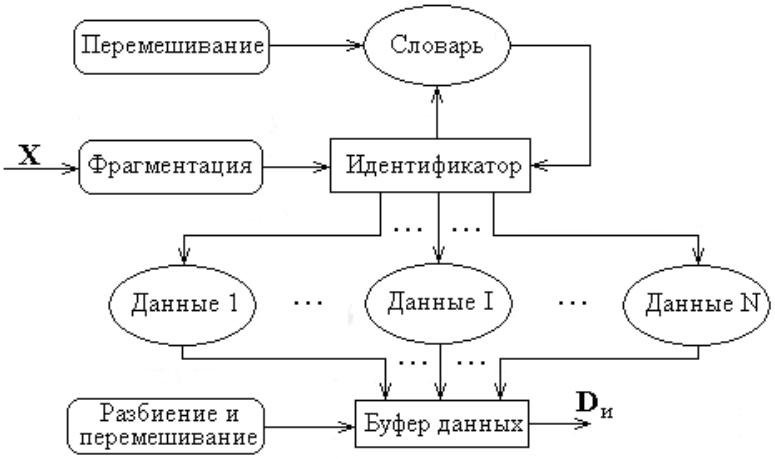


Рисунок 1 — Схема кодирования источника сообщений

Исходный текст **X** разбивается на фрагменты $\mathbf{X_J}$. Идентификатор осуществляет последовательное сравнение элементов $\mathbf{X_J}$ со словарем, который составляется на основе анализа текстов, относящихся к определенной предметной области. Каждому элементу словаря соответствует номер ячейки, в которой этот элемент хранится. На выходе идентификатора формируется последовательность двоичных адресов ячеек словаря $\mathbf{D_{J1}}$. Упорядоченное множество $\mathbf{D_{J2}}$ содержит фрагменты адресов из множества $\mathbf{D_{J1}}$ после их разбиения и последующего перемешивания. Выходное множество данных $\mathbf{D_и}$ формируется из элементов множества $\mathbf{D_{J2}}$, последовательно объединяемых в блоки одинаковой длины *l*, которая равна длине адреса ячейки словаря. В случае разбиения исходного текста на k фрагментов осуществляются (k-1) перемешивание словаря и (k-1) разбиение и перемешивание фрагментов адресов.

Применяемые алгоритмы перемешивания и разбиения адресов словаря должны быть указаны в ключе, передаваемом вместе с данными по КС. Предлагаемая схема позволяет установить однозначное соответствие последовательности элементов исходного сообщения данным из множества $\mathbf{D_и}$ и обратное преобразование данных в текст с графиком обратного соответствия $\mathbf{Q^{-1}} \subseteq \mathbf{D_и} \times \mathbf{X}$.

В рассматриваемом методе кодирования «случайным» образом изменяется порядок следования символов, служащих для обозначения элементов исходного сообщения. В качестве кодов используются адреса ячеек словаря, причем адреса ячеек, содержащие элементы исходного сообщения, могут отсутствовать в передаваемых данных. Предварительно можно рекомендовать использовать данный метод для конфиденциальной передачи небольших текстовых сообщений и архивирования данных.

УДК 621.391

ПУТИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ СЖАТИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ МЕТОДАМИ СЕМЕЙСТВА LZ

Кравченко В. В., аспирант
Севастопольский национальный технический университет, e-mail: vovchik33@km.ru

Практически все словарные кодировщики принадлежат семейству алгоритмов, происходящих из работы Зива и Лемпеля. Преимуществом методов данного семейства является умение быстро приспосабливаться к структуре текста. С точки зрения практического применения алгоритмов семейства LZ важно отметить вниманием решение следующих вопросов: как организовать хранение в памяти кодера и декодера большого словаря, составленного из слов различной длины; как поступать при заполнении этим словарем всего допустимого объема памяти; как оптимизировать заполнение словаря, увеличив скорость и эффективность его обучения.

Решение способа организации хранения словаря в работах Велча предложено в виде представления словаря в качестве дерева, что позволяет поиск сделать достаточно быстрым. Дополнительное ускорение поиска возможно за счет использования хеширования. Решение проблемы переполнения словаря возможно несколькими вариантами: прекращение наращивания словаря (LZW); полный сброс памяти и возвращение алгоритма к начальному состояния (LZC); сброс наименее используемой в последнее время фразы – LRU-замещение (LZT). Еще один способ,

частично решающий проблему переполнения словаря – динамическое расширение области памяти по мере заполнения текущего словаря. Такой способ позволяет алгоритму самому выбирать длину кодовой комбинации в зависимости от степени заполненности словаря. Однако, следует помнить, что расширение словаря приводит к снижению скорости поиска его элементов. На практике размер словаря определяется длинной указателя, максимальное значение которого обычно составляет 16 бит.

Увеличение скорости обучения словаря возможно двумя путями: предварительная загрузка словаря – имеющегося либо сформированного в результате обработки исходного текста; использование подхода, предложенного в реализации метода LZMW, который предполагает формирование новой фразы путем конкатенации последних двух кодированных фраз вместо добавления к существующей фразе одного символа (LZW). Такие стратегии – загрузка внешнего словаря и быстрое конструирование – позволяют достигать лучшего сжатия, но требуют продуманной структуры данных. Кроме того, более быстро происходит переполнение словаря.

С целью повышения эффективности экономного кодирования текстовых данных методами семейства LZ предлагается оптимизировать заполнение словаря за счет учета грамматики языка – а именно морфологии и синтаксиса. Формирование новой фразы словаря может осуществляться любым из способов, предложенных в методах LZW и LZMW. Выбор метода определяется грамматическими особенностями текущей и предыдущей кодируемых фраз. Для этого предлагается оптимизировать структуру словаря таким образом, чтобы для каждой фразы было известно, каким из двух способов, возможно формирование новой фразы на основе текущей.

УДК 621.382

АДАПТИВНЕ ЗМЕНШЕННЯ НАДЛИШКОВОСТІ ДАНИХ НА БАЗІ ПОЛІНОМНИХ МЕТОДІВ ПЕРЕДБАЧЕННЯ ТА ІНТЕРПОЛЯЦІЇ

Ю.Ю. Іляш, аспірант
Прикарпатський Національний університет імені Василя Стефаника, e-mail: yurchukil@gmail.com

В техніці з моменту її зародження актуальною проблемою є максимальне зменшення об'єму сигналу, що передається, без втрат його інформаційного змісту.

Одним з ефективних методів рішення цієї проблеми є скорочення природної надлишковості, тобто "ущільнення". Основний принцип, на якому базується ущільнення даних, полягає в економічному описі повідомлення, згідно якому можливе відновлення початкового його значення з похибкою, яка контролюється.

Алгоритми ущільнення з втратами призначені для зменшення надлишковості інфопотоків за рахунок видалення з вхідного повідомлення неістотних відліків у певні моменти часу; для чого на початковому етапі вхідний сигнал рівномірно дискретизується і представляється послідовністю відліків $\{y_i\}$, де i – час або номер відліку.

Задача стиснення полягає в частинній апроксимації вхідних даних довільною функцією заданої форми. Очевидно, що у відновлений процес вноситиметься похибка, оскільки точні значення y_i замінюють на

наближені y_i за умови, що $\left|y_i - \hat{y}_i\right|$ не перевищує заданого значення гранично допустимої похибки ε.

Як апроксимуючу функцію найчастіше використовують многочлен m-го степеня

$$y(i) = b_0 + b_1 i + b_2 i^2 + ... + b_n i^n, \qquad (1)$$

тому алгоритми, які використовують для апроксимації процесу лінійні многочлени, називаються поліномними.

Методи, які використовують інші види апроксимуючих функцій, наприклад синусоїдні чи експоненціальні, відрізняються складністю і у більшості випадків поступаються за ефективністю поліноміальним алгоритмам.

Поліноміальні алгоритми, які в процесі зменшення надлишковості інфопотоків відкидають значну частину відліків, можна поділити на два класи: передбачення та інтерполяції. В алгоритмах передбачення апроксимуюча пряма змінює своє положення тоді, коли з поступленням нових відліків виникає перевищення допустимої похибки. У випадку інтерполяції положення апроксимуючої кривої може змінюватись з поступленням наступного відліку.

У результаті огляду існуючих методів зменшення надлишковості на базі поліномних алгоритмів передбачення та інтерполяції виявлено особливості кожної модифікації алгоритму та принципи відбору істотних відліків. Проведено аналіз побудови та зміни апертури допуску у відповідності до характеристики отриманого відліку.

В подальшому доцільно звернути увагу на визначення ефективності компресії розглянутих алгоритмів при застосуванні до сигналів різних форм. Зважаючи на те, що значну частину обсягу стиснутих даних займає саме службова інформація, слід звернути увагу на дослідження ефективності часової синхронізації істотних відліків.

УДК 681.322:621.391

МЕТОД ТАЄМНОЇ ПЕРЕДАЧІ ДАНИХ НА ОСНОВІ ФРАКТАЛЬНОГО АЛГОРИТМУ УЩІЛЬНЕННЯ ЗОБРАЖЕНЬ

А.С. Васюра, к.т.н., професор,
e-mail: vasanat@inaeksu.vstu.vinnica.ua
Є.А. Золотавкін, аспірант,
Вінницький національний технічний університет
e-mail: zhzolot@rambler.ru

Сьогодні тайнопис реалізується різними способами. Загальною рисою цих способів є те, що приховане повідомлення вбудовується в деякий об'єкт, що не привертає уваги. Вбудовування таємної інформації в класичній стеганографії відбувається шляхом деякої зміни об'єкта, в який вона вбудовується. Надійність стеганографічного каналу прямо залежить від ступеня складності виявлення змін внесених в об'єкт.

Значними перевагами володіють методи, що використовують особливості алгоритмів ущільнення зображення з втратами. В такому випадку вибір алгоритму ущільнення вказує ідею вбудовування даних.

Фрактальний алгоритм стиснення зображень є перспективним з точки зору стеганографічного використання так як демонструє високу ефективність: залежність між коефіцієнтом ущільнення та якістю відновленого зображення інтерпретується експертами як одна з найкращих.

Метою фрактального алгоритму ущільнення є пошук сукупності перетворень для деякого оригінального зображення, що забезпечує достатній ступінь подібності відновленого зображення з оригіналом. Однак така сукупність не задається однозначно. Можливість

маніпулювання сукупністю в межах допустимих відхилень від оригіналу дозволяє застосовувати стеганографічну техніку. Особливістю такого метода вбудовування даних є різноманіття взаємозамінних фрагментів реальних зображень.

Запропоновано ідею вбудовування, що використовує властивості фрактального алгоритму ущільнення зображень. Ідея стеганографічного використання фатального алгоритму, описана в попередніх роботах, полягає у процедурі невипадкового вибору доменного блоку (у якості відповідника ранговому) з певної сукупності подібних доменних блоків.

Враховано особливості сучасних реалізацій фрактального алгоритму. Під час проектування необхідно враховувати всі особливості алгоритму ущільнення з метою створення ефективного методу приховування даних, позбавленого демаскуючих ознак. Такі особливості визначаються не тільки вибором алгоритму ущільнення, але й удосконаленнями, що покликані підвищити його ефективність.

Беручи до уваги основні тенденції розвитку сучасних фрактальних алгоритмів ущільнення зображень, можна виділити фрагменти, запозичення яких дозволить мінімізувати час. Такі фрагменти можна класифікувати, опираючись на стеганографічну значимість виконуваних операцій, що дозволить розробити пристосований стегометод.

З метою адаптації ідеї до умов незначних спотворень, передбачених фрактальним алгоритмом, запропоновано вивчати та використовувати властивості множини доменних блоків за допомогою методів кластеризації.

Опираючись на особливості запропонованого стегометоду, розроблено стеганографічний критерій, що дозволить контролювати використання доменних блоків з метою позбавлення демаскуючих ознак.

УДК 681.322:621.391

ВДОСКОНАЛЕННЯ МЕТОДА ВБУДОВУВАННЯ ДАНИХ НА ОСНОВІ АЛГОРИТМУ ВЕЙВЛЕТ-УЩІЛЬНЕННЯ ЗОБРАЖЕНЬ

А.С. Васюра, к.т.н., професор,
e-mail: vasanat@inaeksu.vstu.vinnica.ua
В.В. Лукічов, здобувач,
Вінницький національний технічний університет
e-mail: lukitchov@mail.ru

В даний час у зв'язку з бурхливим розвитком обчислювальної техніки і нових каналів передачі інформації з'явилися нові стеганографічні методи, в основі яких лежать особливості представлення інформації в комп'ютерних файлах, обчислювальних мережах і т.п.

Стеганографія займає своє місце в забезпеченні безпеки: вона не заміняє, а доповнює криптографію. Приховання повідомлення методами стеганографії значно знижує ймовірність виявлення самого факту передачі повідомлення. А якщо це повідомлення до того ж зашифроване, то воно має ще один, додатковий, рівень захисту.

Реальні зображення зовсім не є випадковим процесом з рівномірно розподіленими значеннями величин. Добре відомо, і це використовується в алгоритмах стиску, що більша частина енергії зображень зосереджена в низькочастотній частині спектра. Звідси і потреба в здійсненні декомпозиції зображення на субсмуги. Далі стегоповідомлення повинне додаватися до субсмуги зображення. Низькочастотні субсмуги містять величезну частину енергії зображення, отже, носять шумовий

характер. Високочастотні субсмуги найбільш піддані впливу з боку різних алгоритмів обробки, будь то ущільнення або НЧ фільтрація. Таким чином, для вбудовування повідомлення найбільш підходящими кандидатами є средньочастотні субсмуги спектра зображення.

Ефективність застосування вейвлет-перетворення і ДКП для стиску зображень пояснюється тим, що вони добре моделюють процес обробки зображення в системі зору людини, відокремлюють «значимі» деталі від «незначущих». Отже, їх більше доцільно застосовувати у випадку активного порушника. Справді, модифікація значимих коефіцієнтів може привести до неприйнятного перекручування зображення. При застосуванні перетворення з низькими значеннями виграшу від кодування існує небезпека порушення повідомлення, тому що коефіцієнти перетворення менш чутливі до модифікацій. Однак, існує більша гнучкість у виборі перетворення. І якщо перетворення невідомо порушникові, то модифікація стего буде ускладнена.

Вдосконалено стеганографічний метод, що використовує зображення у якості контейнеру. Перетворення з метою вбудовування секретного повідомлення виконуються над вейвлет-коефіцієнтами, що робить метод адаптованим до стиску з втратами сучасними алгоритмами. Експериментальні результати демонструють, що стегозображення візуально не відрізняється від оригіналу та характеризується високим значенням критерію PSNR. Діставання секретного повідомлення здійснюється за допомогою ключа. Однак, метод має абсолютну стійкість лише до JPEG-ущільнення з невеликими коефіцієнтами.

УДК 004.627

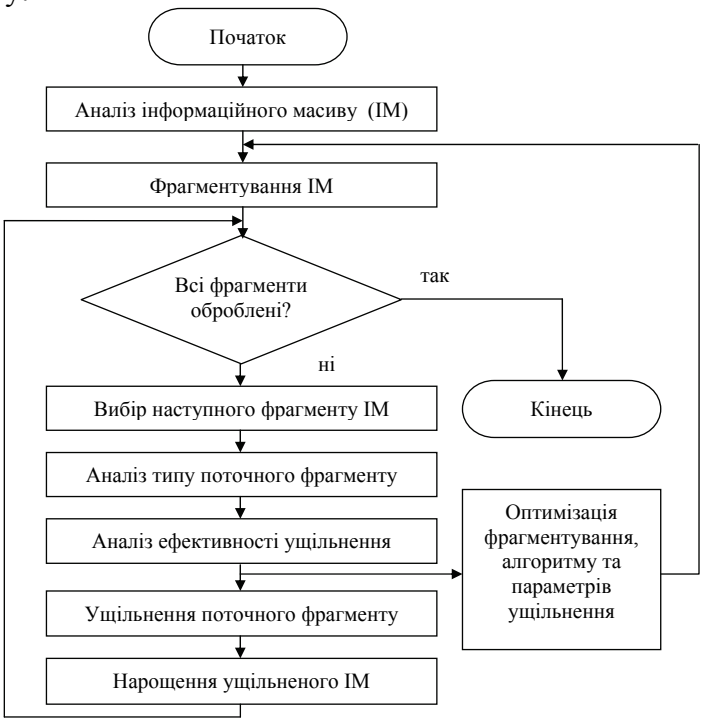
АДАПТИВНІ СИСТЕМИ УЩІЛЬНЕННЯ ІНФОРМАЦІЇ

Ю.С. Балицький, О.В. Губа, І.П. Дробязко
Національний технічний університет України
“Київський політехнічний інститут”
e-mail: may@scs.ntu-kpi.kiev.ua

Незважаючи на стрімке зростання можливостей сучасної комп’ютерної техніки щодо збереження величезних обсягів інформації, задача підвищення ефективності засобів ущільнення інформаційних масивів у жодній мірі не втрачає своєї актуальності. Важливим резервом підвищення ступеня стиснення інформації є удосконалення механізмів пристосування алгоритмічного апарату архіваторів до особливостей конкретного інформаційного масиву.

У доповіді наводяться результати дослідження систем ущільнення даних з можливістю об’єктно-орієнтованої оптимізації. У даному контексті подібні системи можна поділити на два класи: настроювані та адаптивні. Настроюваною (або адаптовною) вважатимемо систему ущільнення, яка має деякий набір змінних параметрів, котрі керують алгоритмом обробки даних, визначаючи таким чином ефективність архівування конкретного масиву. При цьому настроювання відповідних параметрів виконується апріорно тільки один раз перед початком роботи. Адаптивною називатимемо систему, яка здатна до автоматичної оптимізації своїх параметрів щодо конкретного об’єкту архівації та, можливо, деяких зовнішніх факторів (зокрема, корегування критеріїв

оптимізації користувачем). Доповідь містить докладний опис архітектурної організації адаптивного архіватора даних, розробленого авторами. Узагальнений алгоритм функціонування програмного інструменту подано на рисунку.



У доповіді наводиться аналіз ефективності застосування у архіваторі кількох стандартних методів стиснення даних. Дана статистика результатів архівування файлів різних типів, а також змішаних (щодо типу даних). За результатами експериментів адаптивний архіватор порівнюється з рядом найпоширеніших програмних продуктів аналогічного призначення. При цьому використовується комбінований критерій ефективності, котрий враховує швидкодію та ступінь стиснення.

УДК 004.056

СПОСІБ УЩІЛЬНЕННЯ ОСТЕОСЦИНТИГРАФІЧНИХ ЗОБРАЖЕНЬ

Д.С.Замятін, к.т.н., О.С.Кебкало, О.Ю.Наливайчук
Національний технічний університет України
"Київський політехнічний інститут"
e-mail: may@scs.ntu-kpi.kiev.ua

Єдиним засобом достовірної діагностики ряду серйозних захворювань кісткової системи на сьогоднішній день є остеосцинтиграфія. Однак її широке застосування в традиційній медичній практиці ускладнюється відсутністю достатньої кількості висококваліфікованих вузькопрофільних фахівців. Ефективною формою впровадження багатьох нових медичних технологій є телемедицина, але застосування остеосцинтиграфії в теледіагностиці стримується складністю передачі в реальному часі величезних обсягів цифрових остеосцинтиграфічних зображень.

У доповіді пропонується новий спеціалізований спосіб ущільнення остеосцинтиграфічних зображень на основі дискретного косинусного перетворення. Наводиться оригінальний критерій оцінки втрат діагностичної якості зображень, орієнтований на клас остеосцинтиграфічних знімків. Запропоновано спеціалізований протокол передачі остеосцинтиграфічних даних з можливістю вибору ступеню ущільнення зображення до 60 разів без суттєвих втрат діагностичної якості. У доповіді подається опис структурної та алгоритмічної організації системи телемедичної системи обробки остеосцинтиграм, наводяться результати дослідного впровадження системи.

УДК 681.3

КЛАСИФІКАЦІЯ СИСТЕМ, В ЯКИХ ВИКОРИСТОВУЄТЬСЯ УЩІЛЬНЕННЯ ДАНИХ

В. А. Лужецький, д.т.н., професор
Вінницький національний технічний університет,
М.В. Моторний, аспірант
Aldec-ADT sp. z o.o., Катовіце, Польща

Будь-який метод ущільнення містить два види перетворень: ущільнення і відновлення. Ці перетворення можуть здійснюватися на основі різних функцій відображення, причому реалізація кожної з функцій ущільнення має деяку обчислювальну складність C_c, вимагає деякого об'єму пам'яті V_c і забезпечує коефіцієнт ущільнення k. У свою чергу, реалізація перетворення відновлення має обчислювальну складність C_d і вимагає об'єму пам'яті V_d. Час оброблення тексту залежить від обчислювальної складності реалізації ущільнення і відновлення.

Системи, в яких використовується ущільнення, висувають різні вимоги до методів ущільнення. Вводяться такі класифікаційні характеристики: швидкість ущільнення і відновлення – F (Fast, швидке), S (Slow, повільне); об'єм пам'яті, необхідної для реалізації ущільнення і відновлення – L (Limited, обмежений), U (Unlimited, необмежений); коефіцієнт ущільнення – H (High, високий), D (Don't care, не має значення).

Виходячи з даних характеристик, пропонується класифікація систем, в яких використовується ущільнення та наводяться приклади систем, що використовують ущільнення, ґрунтуючись на їхніх класифікаційних

характеристиках: FUDSU – система резервного копіювання; SUDFU – репозиторій бази даних; FUDFU – система, що включає в себе відносно швидкий канал передавання даних; FLDSU – система, у якій здійснюється передавання даних з малопотужного мобільного пристрою на настільну робочу станцію; SUDFL – система, у якій здійснюється передавання даних з настільної робочої станції на малопотужний мобільний пристрій; FLDFL – система, у якій здійснюється передавання даних з одного малопотужного мобільного пристрою на інший; SUHSU – система, у якій здійснюється передавання даних у каналі з низькою пропускною здатністю з однієї настільної робочої станції на іншу; SUHFU – система, у якій здійснюється передавання даних у каналі з низькою пропускною здатністю з потужного сервера на настільну робочу станцію (Інтернет з модемним з'єднанням).

З метою обрання серед наявних методів ущільнення оптимального методу для даної системи, необхідно визначити критерій ефективності ущільнення. Такий критерій для *i*-го методу визначається за формулою:

$$E_i = \omega_1 \cdot \delta C_{C_i} + \omega_2 \cdot \delta V_{C_i} + \omega_3 \cdot \delta k_i + \omega_4 \cdot \delta C_{D_i} + \omega_5 \cdot \delta V_{D_i}$$

де δC_c – відносна обчислювальна складність ущільнення, δV_c – відносний об'єм пам'яті для ущільнення, δk – відносний коефіцієнт ущільнення, δC_d – відносна обчислювальна складність відновлення, δV_d – відносний об'єм пам'яті для відновлення, ω_j – вага *j*-ої характеристики, що вибирається з урахуванням вимог до системи, у якій використовується ущільнення.

Запропонована класифікація систем, що використовують ущільнення даних, дозволяє висунути обґрунтовані вимоги до методу ущільнення, а критерій ефективності дозволяє сформулювати і розв'язати задачу вибору оптимального методу ущільнення.

УДК 681.3

КОДУВАННЯ ДЖЕРЕЛ ДАНИХ БЕЗ ПАМ'ЯТІ З ВИКОРИСТАННЯМ СКОРОЧЕНИХ ФОРМ Р-КОДІВ ФІБОНАЧЧІ

В. А. Лужецький, д.т.н., професор,
І.В. Бугорська, студентка,
Вінницький національний технічний університет

Для ущільнення потоку цілих чисел застосовуються методи, що базуються на відокремленні мантис і експонент (SEM-методи). При цьому підвищення ступеня ущільнення досягається використанням кодів змінної довжини (кодів Еліаса, Райса, Голомба, Фібоначчі).

У доповіді розглядаються скорочені форми узагальнених кодів Фібоначчі, які забезпечують ущільнення потоку цілих чисел.

Існує множина форм *p*-кодів Фібоначчі, серед яких є єдина форма, в який праворуч від кожної одиниці розташовано *p* або більш нулів. Вона називається *мінімальною формою* (М-*формою*).

Форма коду, що отримана з М-форми шляхом відкидання *p* нулів праворуч від кожної одиниці, називається *скороченою формою першого типу* (C_1-*формою*).

Оскільки C_1-форми різних кодів мають різну розрядність, то у процесі їх перетворення в М-форму виникає необхідність визначення початку або закінчення кожного коду. Це відбувається таким чином. Починаючи зі старших розрядів, здійснюється лічба кількості розрядів з урахуванням записів *p* нулів після кожної одиниці. Як тільки підрахована кількість розрядів стане дорівнювати *n*,

формується ознака закінчення одного коду і початок наступного.

Форма коду, що отримана з М-форми шляхом відкидання усіх нулів старших розрядів до першої одиниці, називається *скороченою формою другого типу* (C_2-*формою*).

Оскільки C_2-форма задовольняє ознаці М-форми, то на межі двох C_2-форм необхідно розмістити групу символів, яка не задовольняє цій ознаці. Для цього пропонується записувати символ 1 в наймолодший розряд C_2-форми *p*-коду. Ознаками межі між двома кодами є наявність двох одиниць у сусідніх розрядах для $p>1$ і двох чи трьох одиниць для $p=1$.

Форма коду, що отримана з М-форми шляхом відкидання усіх нулів молодших розрядів, крім одного, до першої одиниці, називається *скороченою формою третього типу* (C_3-*формою*).

Для того, щоб забезпечити відокремлення кодів в самий молодший розряд записується символ 1. Ознакою межі кодів є наявність у сусідніх розрядах або двох, або трьох одиниць..

Форма коду, що отримана з М-форми шляхом відкидання однакової кількості нулів до першої молодшої одиниці і до першої старшої одиниці, називається *скороченою формою четвертого типу* (C_4-*формою*).

Для забезпечення можливості відокремлення кодів у кожному з них ліворуч від першої старшої одиниці і праворуч від першої молодшої одиниці має бути розташований хоч би один нуль і в самий молодший розряд потрібно записати символ 1. Ознакою межі кодів є наявність у сусідніх розрядах двох одиниць..

Скорочені форми *p*-кодів Фібоначчі розширюють клас кодів змінної довжини і забезпечують підвищення ступеня ущільнення потоку цілих чисел.

УДК 621.39

АВ-СЖАТИЕ ДВОИЧНОЙ ИНФОРМАЦИИ

А.А. Борисенко, д.т.н., профессор,
И.А. Кулик, к.т.н., доцент
Сумский государственный университет
e-mail: electron@sumdu.edu.ua, kulik@pe.sumdu.edu.ua

Использование средств сжатия данных в электронных системах обеспечивает увеличение их производительности за счет уменьшения времени передачи информации, а также снижает требования к емкости памяти. Особое значение приобретают методы сжатия, которые, с одной стороны, позволяют осуществлять обработку информации в реальном времени, а, с другой, выполнять сжатие без информационных потерь. Такие методы могут эффективно применяться в информационных системах, где психофизиологический фактор сведен к минимуму, а ценность данных является высокой.

Одним из таких сжимающих методов является метод АВ-сжатия двоичной информации. Метод кодирования f_{av}, который заключается в переходе от векторного представления двоичных слов к адресному в зависимости от числа k единиц в исходном слове $a_i \in A$ согласно условию

$$\begin{cases} 0 \le k < \alpha - 1 \\ n - \alpha + 1 < k \le n \end{cases}, \text{ где } \alpha = n / \lceil \log_2 n \rceil,$$

называется методом АВ-сжатия, а получаемый код – АВ-кодом. Элементы АВ-кода образуются согласно правилу:

$$f_{av}(a_i) = \begin{cases} \{\mathrm{Bin}\, k, VU(a_i)\}, 0 \le k < \alpha - 1 \\ \{\mathrm{Bin}\, k, VZ(a_i)\}, n - \alpha + 1 < k \le n \\ \{\mathrm{Bin}\, k, a_i\}, \alpha - 1 \le k \le n - \alpha + 1 \end{cases},$$

где A – исходное множество двоичных n-разрядных слов a_i,

$i=1,\ldots,|A|$; $VU(a_i)$ и $VZ(a_i)$ – векторы двоичных адресов единиц и нулей слова a_i; Bin k – двоичная запись числа k единиц исходного слова.

Область использования АВ-сжатия двоичных слов, генерируемых источником информации Бернулли:

$$\begin{cases} 0 \le p < 1/\lceil \log_2 n \rceil - 1/n + \gamma/n \\ 1 - 1/\lceil \log_2 n \rceil + 1/n - \gamma/n < p \le 1 \end{cases},$$

где p – вероятность появления двоичной единицы; γ – допустимое заданное отклонение случайной величины k.

Алгоритмы, лежащие в основе метода АВ-сжатия, строятся на основе достаточно простых процедур: подсчет числа двоичных единиц и формирование адресов.

Средняя длина кодовых слов, генерируемых источником Бернулли, после АВ-сжатия определяется как

$$C(f_{av}) = \sum_{k=0}^{\alpha-2} P_k (k+1)\lceil \log_2 n \rceil + \sum_{k=\alpha-1}^{n-\alpha+1} P_k \left(n + \lceil \log_2 n \rceil\right) + \\ + \sum_{k=n-\alpha+2}^{n} P_k (n-k+1)\lceil \log_2 n \rceil ,$$

а среднее время работы сжимающего алгоритма (без использования кодовых таблиц)

$$V = V_c + \sum_{k=0}^{\alpha-2} P_k \frac{k(n+1)}{(k+1)} + \sum_{k=n-\alpha+2}^{n} P_k \frac{(n-k)(n+1)}{(n-k+1)},$$

где V_c – время подсчета двоичных единиц; P_k – вероятность появления числа k единиц.

Таким образом, метод АВ-сжатия при достаточно хорошей степени сжатия обладает следующими достоинствами:

- высокая скорость работы алгоритмов сжатия и восстановления данных;
- малый уровень аппаратно-программных затрат при практической реализации.

УДК 004.627

ПРИМЕНЕНИЕ АЛГОРИТМОВ БИНОМИАЛЬНОГО СЧЕТА ДЛЯ СЖАТИЯ ДВОИЧНЫХ КОДОВ

А. А. Борисенко, д.т.н., профессор,
Сумский государственный университет
e-mail: electron@sumdu.edu.ua;
В. Б. Чередниченко, ст. преподаватель,
Харьковский национальный университет внутренних дел, факультет в г. Сумы, e-mail: chered_ukr@ukr.net

При обработке данных в электронных системах часто используется сжатие различной информации.

Ранее были описаны алгоритмы биномиального счета, которые отличаются простотой и эффективностью при сжатии равновесных кодов. Предложены формулы для оценки времени преобразования и коэффициента сжатия в случаях одинаковой и различной вероятности появления кодовых комбинаций.

Предлагается использовать данный метод для сжатия любых двоичных кодов длиной n. Здесь каждую из исходных кодовых комбинаций можно считать отдельной равновесной комбинацией длиной n, для чего запоминать количество единиц k, присущее только ей. Сжатие состоит в преобразовании исходной комбинации в биномиальный код методом отбрасывания определенного числа единиц или нулей, а затем в преобразовании этой последовательности в номер методом биномиального вычитающего счета.

Коэффициент сжатия равновесных кодов $\boldsymbol{Y}$ равен:

$$\boldsymbol{Y = log_2 C_n^k / n} \qquad (1)$$

где n – длина кодовых комбинаций,

k – число единиц в комбинации.

Произвольная двоичная комбинация после сжатия будет содержать ее номер и дополнительные данные о количестве единиц в ней $q = \log_2 n$. Тогда коэффициент сжатия двоичных комбинаций Y^* несколько уменьшится:

$$Y^* = (\log_2 C_n^k + \log_2 n) / n \qquad (2)$$

Оценить среднее количество тактов преобразования исходных кодов в их номера при равновероятном появлении каждой комбинации можно по формуле:

$$\overline{N} \approx \frac{C_n^k - 1}{2} + n, \qquad (3)$$

Погрешность расчетов при n >6, k >1 не превышает 8%. Первое слагаемое является определяющим начиная с k >2.

Количество тактов преобразования можно уменьшить, используя свойства пары двойственных биномиальных систем, построенных на известном соотношении $C_n^k = C_n^{n-k}$.

Имеется способ дальнейшего ускорения процедуры сжатия. Проведенные расчеты показывают, что в окрестности точки $k = n/2$ расположен интервал значений k, внутри которого сжатия не происходит. Учитывая это, при количестве единиц в исходной комбинации, соответствующем этому интервалу, целесообразно передавать исходной код, минуя процедуры сжатия. Это не только улучшает характеристики сжатия, но и значительно уменьшает время кодирования, поскольку именно при $k = n/2$ количество тактов преобразования имеет максимум.

Учитывая изложенное, можно на этапе проектирования рационально выбрать интервал параметра k, за счет чего добиться более высокого сжатия при уменьшенных затратах времени на преобразование.

METHOD OF COMPRESSING THE DATA ON THE BASIS OF FIBONACCI P-NUMBERS

Mohammed Abdulkarem Al-Maitah
King Saud University, Kingdom of Saudi Arabia
e-mail: Maitah_mm@hotmail.com

The idea of large integers is the basis of the method of compression in question in the report, In this case the file of data, which must be pressed is considered as one or several large numbers.

The idea of such numbers consists of the following. Integer z is one of the elements of the sequence of integers $\{w_{p,l}\}$, which catches by the recursion relation:

$$w_{p,l} = w_{p,l-1} + w_{p,l-p-1}; \quad p \geq 0; \quad l \geq 0$$

with determined the values initial the elements of $w_{p.0}, w_{p.l}, \ldots, w_{p.p}$.

The direct calculation of the element of sequence is achieved according to the formula:

$$w_{p,l+2p} = w_{p,p}\varphi_p(l+p) + \sum_{i=0}^{p-1} w_{p,i}\varphi_p(l+p-i-1),$$

where $\varphi_p(k)$ - k-e Fibonacci p-number.

Based on this, the task of the idea of integer z consists in the determination of the integer values, the initial elements of sequence $\{w_{p,l}\}$ and number of the element, which is equal to z, I.e. any integer is represented in the form:

$$z = \sum_{i=1}^{p+1} q_i \varphi_p(j+i-1), \qquad (1)$$

where q_i the integers; $j = 0, 1, 2, ...$

Collection $\{q_1, q_2, \cdots, q_{p+1}, j\}$ is called the q-representation of the number z.

There are many representations of the form (1), but for the task of compressing the data it is expedient to use an idea, which has the following property $\{\min|q_i|; i = 1,2,\cdots,p+1\}$. This q-representations of integer is called minimum representations . It can have the following structures.

The structure with the fixed boundaries, in which the code length of its component parts does not change, takes the form:

q_1	q_2	...	q_{p+1}	j

However, this form does not always ensure the effective use of bits of the code. For example, for the record of code 00..0010 sufficiently only two bits, and elder zero can be rejected. This leads to the need for the indication of the boundaries between the separate codes.

Structure with the numerical indicators of the floating boundaries between its parts takes the form:

q_1	q_2	...	q_{p+1}	j	n_1	n_2	…	n_p	n_{p+1}

Indicators from the first on p show the boundaries between all q_l, and indicator p+1 - boundary for j

Structure with the code indicator of the floating boundaries between its parts takes the form:

q_1	q_2	...	q_{p+1}	j

For image q_l and j is used the reduced form (C-form) of the p-code. This form is obtained from M-form by the rejection of all zero high-order digits.

УДК 621.396.96

СХЕМА ЛАПЛАСА ПРИ УЩІЛЬНЕННІ ЗОБРАЖЕНЬ

В. П. Майданюк, к.т.н., доцент
Винницкий национальный технический університет,
e-mail: maydan2000@mail.ru

Ефективне кодування зображень ґрунтується на представленні зображення в вигляді декількох компонент з наступним зменшенням точності представлення компонент, але так, щоб виконувались задані вимоги до якості зображення.

Одним з методів, який застосовується для виконання розкладу зображення на компоненти є пірамідальні схеми Лапласа. Сигнал пропускається через фільтр низької частоти B(w) і потім проріджується. В результаті формується низькочастотна субсмуга W_0. Високочастотна субсмуга W_1 формується за рахунок послідовного виконання наступних операцій: інтерполяції W0, згортки з інтерполюючим фільтром A(w) і віднімання результату з початкового сигналу. Реконструкція сигналу відбувається шляхом інтерполяції W0, згортки з інтерполюючим фільтром A(w) і додавання до W1 . Відновлений сигнал точно відповідає початковому, незалежно від вибору фільтрів A(w) і B(w). Повна піраміда будується рекурсивно, із застосуванням наведеної схеми до низькочастотної субсмуги.

Важливою перевагою піраміди Лапласа є багатомасштабність представлення. Зображення представляється одночасно на декількох рівнях з різною роздільною здатністю. Такий підхід дозволяє здійснювати

прогресивну передачу зображення по каналу з обмеженою пропускною спроможністю. При цьому спочатку передається найгрубіше наближення (низькочастотна частина), а потім передаються деталі, від рівня до рівня.

При технічній реалізації цифрових кодуючих пристроїв на основі схеми Лапласа особливий інтерес викликає аналіз зображення квадратними аналізуючими апертурами з розмірами сторін кратними 2^n, оскільки це значно зменшує обчислювальні затрати. Аналіз кореляційних залежностей зображення показує, що збільшення максимального розміру аналізуючих апертур з 8 до 16 не дає помітного виграшу коефіцієнта стиснення. Тому різницеве рівняння, яке описує двовимірний низькочастотний фільтр з найбільшим розміром апертури приймає такий вигляд:

$$H(Z_1,Z_2)=[\frac{1}{4}*(1+Z_1^{-1})(1+Z_2^{-1})]*[\frac{1}{4}*(1+Z_1^{-2})(1+Z_2^{-2})]* \quad (1)$$
$$[\frac{1}{4}*(1+Z_1^{-4})(1+Z_2^{-4})].$$

Де Z1 ,Z2 - трансформоване представлення затримки на рядок зображення та такт дискретизації відповідно. З цього виразу видно, що для формування згладжених компонент для різних розмірів аналізуючих апертур можна використовувати відповідні відводи згладжувального фільтра з найбільшою аналізуючою апертурою.

Таким чином формування низькочастотних компонент зображення зводиться фактично до каскадного з'єднання одновимірних фільтрів з елементами затримки на такт, два такти, чотири такти дискретизації і на один, два і чотири рядки зображення. Операції ділення при виконанні обчислень можуть бути замінені операціями зсуву.

УДК 681.32

ШИФРОВАНИЕ ДАННЫХ ПРИ ИХ СЖАТИИ

В. П. Майданюк, к.т.н., доцент
Винницкий национальный технический университет
e-mail: maydan2000@mail.ru

Основной целью кодирования или сжатия данных является превращение входного потока символов в поток битов минимальной длины. Однако, при сжатии данных некоторыми методами существует возможность одновременного шифрования данных почти без дополнительных вычислительных затрат.

Среди известных алгоритмов сжатия наибольшие преимущества с точки зрения применения их к шифрованию данных имеют два алгоритма:

- сжатие методом MTF (Move To Front);
- вероятностный метод сжатия.

Основной особенностью этих алгоритмов является формирование таблицы символов перед выполнением сжатия данных. Если сформировать эту таблицу с использованием, например, конгруэнтного генератора псевдослучайных чисел у которого начальное значение равно ключу шифра, а потом выполнить сжатие с использованием одного из этих методов, то получим зашифрованное сообщение. Дополнительные затраты отсутствуют, поскольку генерация символов алфавита выполняется в любом случае. К тому же эти алгоритмы являются адаптивными, то есть не требуют передачи дополнительной информации, которая могла быть использована злоумышленниками для взлома шифра, а также характеризуются простой технической реализацией.

УДК 621.39

УЩІЛЬНЕННЯ МОВНИХ СИГНАЛІВ ІЗ ЗАСТОСУВАННЯМ ВЕКТОРНОГО КВАНТУВАННЯ В СИСТЕМАХ ЦИФРОВОГО ЗВ'ЯЗКУ

О. М. Ткаченко, к.т.н., доцент,
e-mail: ant@vstu.vinnica.ua
О. Д. Феферман, студент,
С. В. Хрущак, студент,
Вінницький національний технічний університет

Ущільнення мовних сигналів у системах цифрового зв'язку дозволяє скоротити обсяги даних, що передаються, зменшити ціни на послуги та збільшити кількість абонентів без розширення частотної смуги каналу. Серед найбільш поширених на теперішній час методів найвищу степінь ущільнення забезпечують методи на основі лінійного прогнозування. На практиці частіше застосовують еквівалентну форму представлення коефіцієнтів лінійного прогнозування у вигляді лінійних спектральних пар (LSP).

Для підвищення степені ущільнення LSP квантують за допомогою таблиць, які називаються кодовими книгами. Скалярні кодові книги не потребують складних обчислень і великих витрат пам'яті. Натомість векторні кодові книги дозволяють досягти більшої степені ущільнення при тій же якості синтезованого звуку, що і скалярні кодові книги. Водночас процес ущільнення мовного сигналу за допомогою векторних кодових книг вимагає більших обчислювальних витрат та більших витрат пам'яті. Крім того, при використанні векторних кодових книг постає задача ефективної організації пошуку найближчого

значення. Якість векторних кодових книг у значній степені залежить від фонетичного матеріалу (тренувальної послідовності) та методів його обробки (методів кластеризації)

Одним з найбільш поширених методів, що застосовуються для побудови векторних кодових книг є LBG. При ініціалізації кодова книга заповнюється початковими значеннями, далі проводиться оптимізація кодової книги. Через те, що результати застосування LBG залежать від початкових значень, занесених у кодову книгу, він має суттєві недоліки, а саме: в кодовій книзі можуть з'явитися центроїди, що відповідають пустим кодовим ділянкам та центроїди, нерівномірно розподілені відносно векторів тренувальної послідовності.

Позбутися цих недоліків дозволяє введення додаткового блоку оптимізації кодової книги. Для цього обчислюються значення показника корисності для кожного центроїда. Далі відбувається зміщення центроїдів з низьким показником до центроїдів з високим показником. Це дозволяє розташувати центроїди більш рівномірно.

При створенні кодових книг застосовується зважена евклідова міра для знаходження відстані між векторами. Зважена міра враховує певні особливості LSP, що дозволяє отримати кращі результати, ніж при використанні звичайної міри.

Для прискорення операції пошуку в кодовій книзі центроїди впорядковуються відносно обраних точок відліку, що дозволяє суттєво прискорити операцію пошуку при незначному погіршенні якості сигналу.

В результаті дослідження було розроблено кодову книгу, що враховує особливості української мови і дозволяє досягти кращої якості синтезованого звука у порівнянні з існуючими кодовими книгами.

УДК 681.39

КЛАСИФІКАЦІЯ МЕТОДІВ УЩІЛЬНЕННЯ, ЩО БАЗУЮТЬСЯ НА ОБЧИСЛЕННІ ВІДХИЛЕНЬ

В.А. Лужецький, д.т.н. професор,
В.А. Каплун, асистент
Вінницький національний технічний університет
e-mail: valuka@rambler.ru

Основні відомі методи ущільнення використовують або статистичні характеристики даних, що ущільнюються, або словниковий принцип. Однак, сучасні мікропроцесори ефективніше здійснюють арифметичні операції над числами. Тому останнім часом здійснюються пошуки підходів щодо ущільнення даних, які базуються на їх представленні як цілих чисел. У доповіді розглядається класифікація методів ущільнення даних, основою яких є обчислення відхилень.

Набір даних, що підлягає ущільненню, можна охарактеризувати діапазоном представлення чисел заданої розрядності, а також такими статистичними параметрами, як мінімальне значення, середнє значення для усього набору або для груп чисел і накопичуване середнє значення для всього набору.

Виходячи з цього, методи ущільнення, що базуються на обчисленні відхилень, можна розділити на дві групи:

- ущільнення з урахуванням статистик;
- ущільнення без урахування статистик.

Серед методів, що здійснюють ущільнення з урахуванням статистичних характеристик, можна виділити такі.

1. Ущільнення, при якому здійснюється розбиття на піддіапазони. У цьому випадку в кожному виділеному піддіапазоні обчислюються відхилення або від центрів

діапазонів, або від середнього значення чисел, що належать даному діапазону. Ущільнена інформація зберігатиметься у такому вигляді: для кожного з відхилень запам'ятовуються знаковий розряд, кількість відкинутих повторюваних старших розрядів, ознака попадання у той або інший піддіапазон. Крім того, для однозначного відновлення первинного вигляду інформації необхідно зберігати самі середні значення чисел у піддіапазоні або числові значення центрів під діапазонів.

2. Ущільнення, при якому вхідний набір чисел розбиваються на групи з n чисел у кожній $(n=2,3,...)$, передбачають обрахування і зберігання або відхилень від середніх значень або б) від мінімальних значень у певній групі. При цьому також для кожного з відхилень зберігаються молодші розряди чисел після відкидання певної кількості повторюваних розрядів і кількість цих відкинутих розрядів. Крім того, у першому випадку слід зберігати знаковий розряд і середнє значення чисел у групі.

3. Ущільнення з урахуванням накопичуваного середнього значення, при якому, зафіксувавши перше число з вхідного потоку даних, обчислюються і зберігаються молодші розряди відхилень від накопичуваного середнього значення. При цьому, окрім самих значень відхилень, необхідно зберігати знаковий розряд і кількість відкинутих повторюваних розрядів.

Серед групи методів, що не передбачають знаходження статистичних характеристик вхідних даних, можна виділити такі: а) ущільнення, основане на зберіганні відхилень від сусіднього елемента; б) відхилення від констант; в) відхилення від відповідних значень апроксимуючої функції. В усіх цих випадках, крім самих відхилень, необхідно зберігати і додаткову інформацію для однозначного подальшого відновлення первинної інформації.

УДК 621.391

УЩІЛЬНЕННЯ СИГНАЛІВ З ДОПОМОГОЮ ЗНАКОЗМІННОГО q-ПЕРЕТВОРЕННЯ

П.В.Козлюк, асистент
Вінницький національний технічний університет
E-mail: kozluk@svitonline.com

Для ущільнення сигналів широко застосовуються методи спектрального аналізу з використанням ортогональних дискретних перетворень(ОДП). При цьому найбільший практичний інтерес представляють ті ОДП, які ділять сигнал на локальні частотні зони і базисні послідовності яких мають локалізацію в часі (наприклад, Wavelet-перетворення).

Відоме q-перетворення, орієнтоване на ефективну обробку сигналів з експоненціальною швидкістю росту.

Матриця q-перетворення має квазитрикутну форму з нульовим правим кутом, елементи a_{ij} якої такі:

$$a_{ij} = \begin{cases} m_i \cdot q^{n_1-(i-1)}, & \mathrm{j} = 1; \\ \mathrm{m_i} \cdot q^{2n_1-(i-j)}, & 1 < \mathrm{j} \le \mathrm{i},\ 1 < \mathrm{i} \le N; \\ -\mathrm{q}^{-1}, & \mathrm{j} = \mathrm{i}+1,\ 1 \le i \le N-1; \\ 0, & \mathrm{j} > \mathrm{i}+1, \end{cases} \qquad (1)$$

де

$$m_i = \begin{cases} 1, & \mathrm{i} < \mathrm{N}; \\ \mathrm{q}^{-\mathrm{n_1}}, & \mathrm{i} = \mathrm{N}. \end{cases}$$

Генерацію базисних послідовностей виконують

задаючи параметр q та визначаючи відповідний параметр n_1 із рівняння:

$$q^{2(n_1+1)} - q^2 + 1 = 0 .$$

Основні властивості q-перетворення:

- ефективний алгоритм швидкого перетворення (рекурентний характер обчислення вимагає тільки два множення і два додавання на один спектральний коефіцієнт не залеж-но від розмірності N);

- довільна розмірність швидкого перетворення;

- мінімальна затримка видачі спектрального коефіцієнта при обробці в темпі надходження вхідних відліків;

- можливість адаптації до сигналу по формі базисних послідовностей шляхом зміни параметра q .

По своїм частотним і кореляційнім властивостям базисні послідовності близькі до широкосмугових сигналів, тобто, q-перетворення не має властивості частотної вибірковості досліджуваного сигналу.

Пропонується розширити набір базисних послідовностей q-перетворення за рахунок зміни, відповідним чином, знаків відліків базисних послідовностей (1).Така зміна знаків дозволяє генерувати декілька твірних базисних послідовностей з різними частотними характеристиками. Наприклад, можна побудувати матрицю q-перетворення , базисні послідовності якої з парними номерами мають частотну характеристику низькочастотного фільтра, а з непарними номерами – частотну характеристику високочастотного фільтра, що дає змогу використати ефективний кратно-масштабний метод ущільнення сигналів.

В доповіді наводяться методики побудови знако-змінних систем базисних функцій q-перетворення.

УДК 681.3

МЕТОД СЖАТИЯ ДАННЫХ С НЕРАВНОМЕРНЫМ РАЗБИТИЕМ НА БЛОКИ

В. А. Лужецкий, д.т.н., профессор,
Адил Ашрафул Хок, аспирант
Винницкий национальный технический университет

Для сжатия данных широко используются методы, учитывающие статистику сообщений, и словарные методы. Однако известные их недостатки стремятся устранить как различными усовершенствованиями, так и поиском принципиально новых подходов к трактовке данных, подлежащих сжатию.

Один из таких подходов заключается в рассмотрении данных, независимо от их фактического содержания, как чисел. При этом файл данных, который необходимо сжать, рассматривается как М-представление нескольких сверхбольших целых положительных чисел одинаковой разрядности (1024 и больше разрядов) линейной формой Фибоначчи. Именно свойство М-представления и обеспечивает сжатие данных.

Экспериментальные исследования метода сжатия с использованием М-представления, проведенные авторами, показали, что коэффициент сжатия существенно зависит от разрядности блоков данных и их содержания. Блоки данных, которым соответствуют числа, сравнимые с числами Фибоначчи, сжимаются с высоким коэффициентом сжатия. Если же число, соответствующее блоку данных, значительно отличается от ближайшего числа Фибоначчи, то такой блок мало сжимается.

Исходя из этого, в докладе рассматривается метод,

который предусматривает разбиение файла данных на блоки различной длинны таким образом, чтобы числа, которые соответствуют их содержанию, имели М-представления, обеспечивающие наперед заданный коэффициент сжатия.

Пусть k - желаемый коэффициент сжатия, n - разрядность блока, тогда разрядность М-представления должна быть

$$n^* = n(1-k). \qquad (1)$$

В предлагаемом методе предусматривается разрядность блока от $n_{\min}$ до $n_{\max}$.

Сначала выбирается блок разрядности $n_{\min}$ и для него вычисляются координаты и индекс М-представления. Если полученная разрядность М-представления не удовлетворяет условию (1), то разрядность блока увеличивается на единицу, и вновь вычисляются координаты и индекс М-представления.

Такие действия выполняются до тех пор, пока либо не будет получено М-представление необходимой разрядности, либо разрядность блока не превысит $n_{\max}$. В последнем случае выбирается тот вариант М-представления, который имеет наименьшую разрядность из всех рассмотренных до этого. Таким образом, разрядность блока данных адаптируется под заданный коэффициент сжатия.

Неравномерность разбития файла данных на блоки обеспечивает увеличение коэффициента сжатия по сравнению с разбитием на блоки одинаковой разрядности, но приводит к увеличению времени сжатия, тогда как время восстановления исходного файла остается одинаковым.

УДК 681.518

ЗАСТОСУВАННЯ УЩІЛЬНЕННЯ ТЕСТОВОЇ ІНФОРМАЦІЇ ДЛЯ ПРИСКОРЕНОГО ДІАГНОСТУВАННЯ ЦИФРОВИХ ПРИСТРОЇВ

Перевозніков С.І., д.т.н., професор,
Озеранський В.С., інженер
Вінницький національний технічний університет
e-mail: admin@vkkep.vin.ua

Серед існуючих систем діагностування цифрових пристроїв певне місце займають системи покомпонентного тестування. Особливість таких систем полягає в тому, що можливість фізичного контактування з внутрішніми контрольними точками (КТ) об'єктів дає змогу реалізовувати різноманітні стратегії пошуку несправностей. Конструктивний доступ лежить в основі композиційного підходу до тестування подібних пристроїв. Так, створюючи незалежні електричні умови захисту елементів за рахунок тимчасової комутації внутрішніх вузлів, створюються структури, які найбільш пристосовані до тестування компонентів схем. Так, належним чином формуються, наприклад, генеруючі та паралельні структури. Перші заощаджують об'єм машинної пам'яті для зберігання тестів, другі – економлять час діагностування створених фрагментів за рахунок меншого числа викликів саме процедур тестування.

Дослідження показали, що процес діагностування компонентів схем, які штучно формуються, можна удосконалити за рахунок прискорення обробки відповідних реакцій в процесі подачі тестових впливів у внутрішні КТ. Це може бути здійснено комутацією підмножини внутрішніх вузлів, які мають однаковий

потенціал напруги, безпосередньо на входи елементів „АБО” чи „І”. При цьому відповідна реакція на виході такого елемента свідчить про справність фрагментів схем. Ефективність такого підходу може бути збільшена за рахунок ущільнення інформації про внутрішні КТ до рівня сигнатур з мінімальною розрядністю.

Аналіз показав, що час такої покрокової обробки інформації визначається кількістю входів і числом вибраних елементів контролю. На цьому базується дві стратегії прискореного тестування: перша передбачає подачу тестових впливів з основного роз’єму, а друга – з внутрішніх КТ. Сам процес діагностування нагадує перевірку справності пристрою на основі аналізу “карти напруг”, коли ефект досягається ущільненням тестової інформації і порівнянням її із згенерованими еталонами тестовими векторами на рівні сигнатур. Розрядність сигнатури визначається кількістю тимчасово введених елементів контролю з боку засобів діагностування. Такий підхід найбільш ефективний в умовах серійного виробництва цифрових пристроїв і може бути застосований будь-якими апаратно-програмними засобами внутрішньосхемного пошуку несправностей.

Дослідженням встановлено, що процес ущільнення діагностичної інформації може бути додатково спрощеним за рахунок зменшення кількості введених елементів контролю з боку засобів діагностування. Це здійснюється шляхом електричного з’єднання множин внутрішніх КТ, які мають рівні напруги в визначений час подання тестових векторів. Такий підхід відноситься, в першу чергу, до вузлів пристроїв, які мають рівень лог.1. Наслідком фізичного замішування сигналів є домінування (при наявності несправності) сигналу лог.0 або лог.1 в протилежному випадку.

4. Методи та засоби перетворення форм інформації

УДК 681.325

АНАЛОГО-ЦИФРОВИЙ ПЕРЕТВОРЮВАЧ З КОРИГУВАННЯМ НЕЛІНІЙНОСТІ У БАЗИСІ УОЛША

В.М. Кичак, д.т.н., професор,
Г.Г. Бортник, к.т.н., доцент,
С.Г. Бортник, студент
Вінницький національний технічний університет
e-mail: bortnykg@mail.ru

Ефективність використання обчислювальних та телекомунікацйних засобів визначається рівнем та перспективами розвитку перетворювачів форми інформації (ПФІ). Найбільш поширеними представниками ПФІ є аналого-цифрові перетворювчі (АЦП), до яких висуваються серйозні вимоги щодо підвищення точності. Одним з основних параметрів АЦП, що впливає на точність є нелінійність.

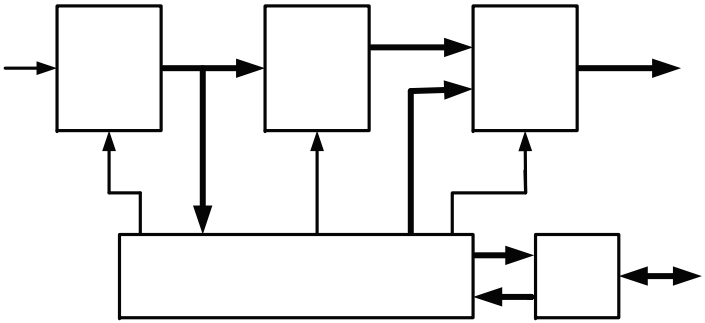
Метою роботи є зменшення нелінійності АЦП шляхом коригування результатів аналого-цифрового перетворення у базисі дискретних функцій Уолша. Для оцінювання нелінійності АЦП використовується гістограмне тестування за допомогою синусоїдального сигналу. При цьому накопичується великий масив даних з виходу АЦП з метою побудови гістограми розподілення значень синусоїдального коливання. На основі гістограми визначається реальна характеристика перетворення АЦП. Виходячи з відомої передатної характеристики, обчислюється інтегральна нелінійність АЦП. Використовуючи значення інтегральної нелінійності, можна виконати діагностування нелінійних властивостей

АЦП на рівні вихідних розрядів. Найбільш оптимальним базисом, у якому можна виконувати таке діагностування є клас дискретних функцій Уолша, які за своїми характеристиками є адекватними для цифрових кодів АЦП. Дискретне перетворення Уолша послідовності $X(n)$, що відображає інтегральну нелінійність, має вигляд

$$X(k) = \sum_{n=0}^{N-1} X(n)\omega al(k,n), \qquad (1)$$

де $\omega al(k,n)$ - дискретні функції Уолша.

Структура спектра у базисі Уолша, отриманого згідно (1), відображає характер інтегральної нелінійності. На основі спектра Уолша можна знайти компенсувальні значення інтегральної нелінійності АЦП. Структура АЦП, реалізованого на базі даного методу, подана на рисунку.



Аналоговий сигнал надходить на вхід базового АЦП (БАЦП). У режимі калібрування вихідні коди через блок керувння (БК), адаптер зв'язку (АЗ) та шину USB подаються в комп'ютер, де програмно визначаються скориговані значення вихідних кодів АЦП, які потім записуються в постійний запам'ятовувальний пристрій (ПЗП). У робочому режимі вихідні коди БАЦП через буферний регістр (БР) подаються на адресну шину ПЗП. З вихідної шини ПЗП зчитуються скориговані коди АЦП.

УДК 621.391

ЦИФРОВИЙ СКРЕМБЛЕР ГРУПОВОГО СИГНАЛУ БАГАТОКАНАЛЬНИХ СИСТЕМ ЗВ'ЯЗКУ

Г.Г. Бортник, к.т.н., доцент,
О.В. Стальченко, асистент, Челоян В.А., студент
Вінницький національний технічний університет
e-mail: bortnykg@mail.ru

В телекомунікаційних системах знаходять широке використання скремблери, які використовуються для захисту від несанкційованого доступу до інформації. Аналогові скремблери не можуть забезпечити надійного захисту переданих групових сигналів багатоканальних систем зв'язку.

У роботі запропоновано пристрій цифрового скремблювання, який функціонує на базі алгоритмів цифрового оброблення сигналів, а саме: аналого-цифрового перетворення, розділення зчитаного блоку інформації на менші проміжки (слоти), перестановки слотів за певним законом та часової інверсії сигналів.

При перетворенні у цифрову форму вузькосмугових групових сигналів частота дискретизації задається як

$$2\frac{f_H}{n_m+1} \le f_S \le 2\frac{f_L}{n_m}, \qquad (1)$$

де f_H, f_L - максимальна та мінімальна частота у спектрі дискретизованого сигналу;

n_m - порядок субдискретизації.

Значення n_m можуть бути лише цілими числами. Тому можна ввести коефіцієнт $l \ge n_m$, який обмежує порядок субдискретизації. Значення l можна знайти з виразу

$$l = ent\left[\frac{f_L}{\Delta f}\right], \qquad (2)$$

де $ent[x]$ – ціла частина числа x.

Таким чином, частота дискретизації сигналів первинної групи може знаходитись у діапазоні 108...120 кГц, що майже у два рази менше, ніж цього вимагає теорема Котельнікова-Шеннона.

Структурна схема цифрового скремблера сигналів первинної групи подана на рис. 1.

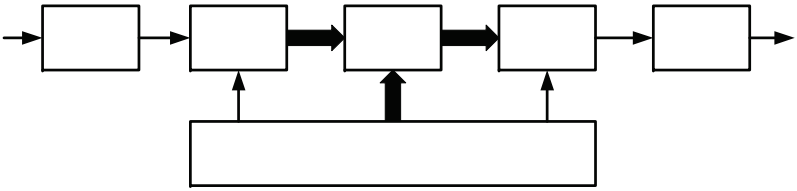


Рис. 1. Цифровий скремблер групового сигналу

Після формування спектра групових сигналів за допомогою фільтра нижніх частот (ФНЧ) та перетворення їх у цифрову форму, оброблювані сигнали з виходу аналого-цифрового перетворювача (АЦП) подаються в оперативний запам'ятовувальний пристрій (ОЗП) статичного типу. Блок керування (БК) формує адреси запису та зчитування даних, а також синхронізує функціонування усіх складових скремблера. В ОЗП сигнал умовно розділяється на блоки однакового об'єму, які потім зчитуються згідно заданого алгоритму криптографічного перетворення. Алгоритм перемішування даних є ключем системи, який зберігається у БК і може змінюватись в залежності від заданих режимів функціонування цифрового скремблера. Перетворення цифрових даних в аналоговий сигнал здійснюється за допомогою цифроаналогового перетворювача (ЦАП) і вихідного ФНЧ.

УДК 621.382(07) + 681.32(07)

АНАЛІЗ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ МЕТОДУ АНАЛОГО-ЦИФРОВОГО ПЕРЕТВОРЕННЯ МОНТЕ-КАРЛО

М.В. Лаврів, асистент
Прикарпатський національний університет
ім. В. Стефаника
e-mail: dlya_marii@mail.ru

За останні роки техніка аналого-цифрового перетворення (АЦП) дозволила значно підвищити рівень техніко-економічних параметрів на потреби користувачів в основному за рахунок технологічних досягнень. Поява нових методів АЦП зумовлена об'єктивними вимогами щодо перетворення форми інформації і в своїй більшості носить характер спеціалізованого призначення. Тенденції розвитку методів та засобів АЦП полягають у скороченні числа інтегральних перетворювачів та переважний розвиток отримають перетворювачі, орієнтовані на застосування із спеціалізованими джерелами повідомлень.

Методи та засоби АЦП відрізняються між собою точністю, швидкодією перетворення, складністю апаратної реалізації і, як наслідок, вартістю. Покращення техніко-економічних характеристик засобів АЦП в основному визначається підвищенням їх швидкодії і розрядності при зниженні собівартості. Одночасно збільшити розрядність і швидкодію дуже складно, оскільки ці параметри є взаємно суперечливими. Збільшення розрядності і, як наслідок, точності перетворення, зумовлює збільшення числа складових пристроїв АЦП або кількості тактів формування відліку, що, в свою чергу, призводить до зниження швидкодії.

З метою підвищення техніко-економічних параметрів засобів АЦП, зокрема розширення частотної смуги вхідного сигналу та уникнення необхідності застосування пристроїв вибірки-зберігання, запропоновано метод статистичних досліджень Монте-Карло, який класифікується до інтегруючих і володіє їх перевагами, зокрема високою точністю перетворення, простотою технічної реалізації та низькими коштами продукції.

Метод Монте-Карло ґрунтується на інтерпретації результату вимірювання як імовірнісного кількісного еквіваленту визначеного роду подій внаслідок статистичних досліджень модельованого процесу, за якими здійснюється обчислення маточікування за частотою (кількістю на періоді дослідження) появи подій внаслідок значної серії незалежних послідовних випробувань.

В порівнянні із методами інтегруючого АЦП метод Монте-Карло, дозволяє значно розширити смугу частотного спектру сигналу перетворення. При цьому точність перетворення зростає пропорційно значенню розрядності коду перетворення та співвідношенню частоти сигналу імовірнісного сканування до частоти верхньої спектральної складової сигналу перетворення.

Досліджено і обґрунтовано ефективність застосуванням методу Монте-Карло на базі генераторів псевдовипадкових послідовностей, що формують сигнал імовірнісного сканування на основі рекурсивних послідовностей максимальної довжини та рандомізованих двійкових кодів. Вперше реалізована можливість і розроблено метод багатоквадрантного перетворення сигналів довільної форми з векторним перемноженням та розділеною індикацією ”+” і ”-” складових, а також як кожного із окремих параметрів, так і проміжних значень їх векторного добутку, графічних одно- та багатоканальних АЦП.

УДК 621.382(07) + 681.32(07)

МЕТОДИ ТА ЗАСОБИ ГЕНЕРУВАННЯ ПСЕВДОВИПАДКОВИХ СИГНАЛІВ ІЗ РІВНОМІРНИМ РОЗПОДІЛОМ

М.В. Лаврів, асистент
Прикарпатський національний університет
ім. В. Стефаника
e-mail: dlya_marii@mail.ru

Реалізація методу статистичних досліджень Монте-Карло передбачає застосування генераторів випадкових значень опорних сигналів із різноманітними законами розподілу, з яких основним є рівномірний розподіл.

У доповіді наведено результати досліджень відомих та запропонованих методів генерування псевдовипадкових чисел, визначення типів розподілів генерованих ними послідовностей, оцінки складності їх технічної реалізації та проаналізовано переваги і недоліки генераторів пседовипадкових чисел.

Застосування методу Монте-Карло до цього часу обмежувалось технічними та алгоритмічними труднощами реалізації якісних і дешевих генераторів псевдовипадкових сигналів із рівномірним розподілом. Розроблено та запропоновано методи формування псевдовипадкових послідовностей на основі кодування Галуа та рандомізації розрядів двійкового коду, для яких наведено алгоритми, методичні та принципові рішення побудови.

Досліджено якісні характеристики рівномірності розподілу запропонованих методів генерування псевдовипадкових чисел за допомогою пакету статистичних тестів *NIST Statistical Tests Suite*, а також

методами χ^2 та Колмогорова-Смірнова.

Отримані результати проведених досліджень дозволили зробити висновок про рівномірний характер розподілу псевдовипадкових чисел та доцільність застосування запропонованих методів для вирішення прикладних задач статистичних досліджень Монте-Карло.

Зокрема, при дослідженні емпіричних розподілів генерованих послідовностей, застосувавши статистичні методи досліджень χ^2 та Колмогорова-Смірнова, найменшим відсотком відхилення від рівномірного розподілу в порівнянні з відомими методами генерування отримав метод перестановки ваги розрядів.

Обґрунтовано ефективність застосуванням методу Монте-Карло на базі запропонованих методів генерування псевдовипадкових послідовностей, що дозволило розробити методи багатоквадрантного перетворення та структури аналого-цифрових перетворювачів двополярних сигналів довільної форми, із векторним перемноженням сигналів, багатоканального та "графічного" перетворення.

Перехід до використання запропонованих методів генерування псевдовипадкових чисел дозволяє значно спростити технічну реалізацію та підвищити якість розподілу випадкових значень генераторів, що дозволило обґрунтувати перспективу застосування методів АЦП Монте-Карло внаслідок досягнення високих показників якості рівномірності псевдовипадкового розподілу при невисокій вартості виготовлення. Із застосуванням імовірнісного методу Монте-Карло на базі запропонованих методів генерування вирішено задачі багатовимірного інтегрування, розроблено алгоритми, програмні моделі та схемотехнічні рішення засобів імовірнісного перетворення форми інформації.

УДК 681.325+681.335

МЕТОД ЗМЕНШЕННЯ ПОХИБКИ КВАНТУВАННЯ В АЦП ПОСЛІДОВНОГО НАБЛИЖЕННЯ НА ОСНОВІ НПСЧ З РОЗРЯДНИМИ КОЕФІЦІЄНТАМИ {1, $\bar{1}$}

С.М. Захарченко, к.т.н., доцент,
О.М. Харьков, аспірант
Вінницький національний технічний університет
e-mail: zahar@vstu.vinnica.ua

Використання алгоритму «тільки включення» в АЦП послідовного наближення на основі НПСЧ має низку переваг, зокрема:

- розширення діапазону вхідного сигналу в зону від'ємних значень ($U_{вх} = \pm U_{оп}$);
- самокомпенсація динамічних похибок, які призводять до помилкового виключення розряду;
- зменшення комутацій ключових елементів за рахунок того, що кожний ключ комутується тільки один раз до $U_{оп}^{+}$ або $U_{оп}^{-}$. Тобто сумарне значення паразитного сигналу, що потрапляє через шину керування також зменшується;
- спрощення процедури формування допоміжного сигналу, оскільки одне і теж значення A_{∂} може використовуватись при калібруванні всіх без винятку „неточних" розрядів.

Одним із головних недоліків згаданого алгоритму є збільшення похибки квантування вдвічі. При використанні системи з розрядними коефіцієнтами {1, $\bar{1}$} залежність

похибки квантування від $A_{вх}$ матиме вигляд, як показано на рис. 1, а, тобто становить ±1 ОМР.

Авторами пропонується використовувати алгоритм „тільки вмикання" з опитуванням компаратору наприкінці останнього, 0-го такту врівноваження. Залежно від його стану додавати або віднімати коригуючу поправку, значення якої становить 0,5 ОМР. Коригуючий сигнал та відкориговану похибку квантування відповідно показано на рис. 1,б та 1,в. Таким чином, похибка квантування після коригування буде в межах ±0,5 ОМР.

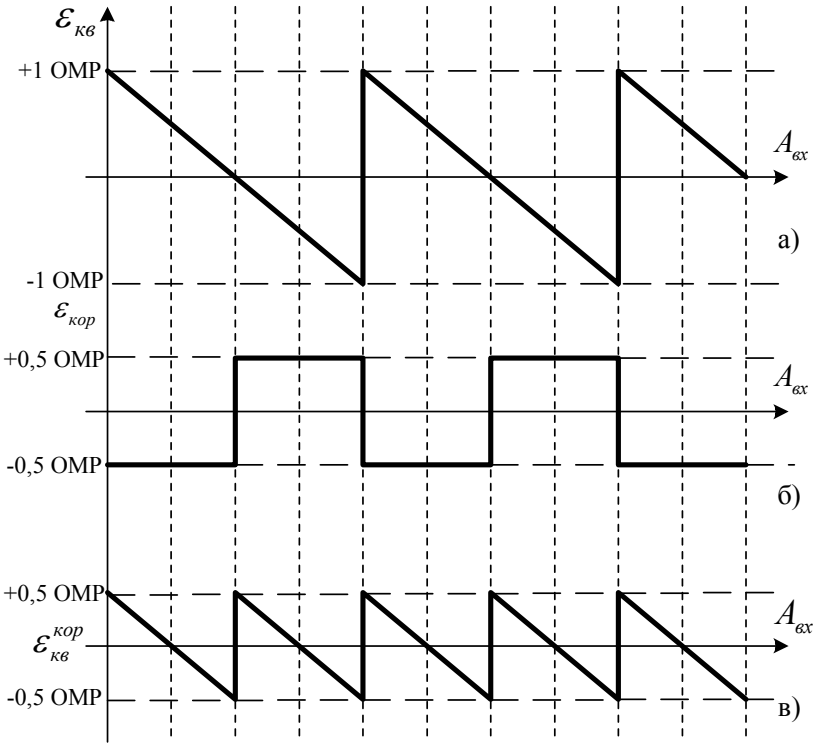


Рис.1 Коригування похибки квантування: а) залежність похибки квантування від $A_{вх}$; б) коригуючий сигнал; в) відкоригована похибки квантування.

УДК 681.317

ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ В ВИМІРЮВАННЯХ З ЧАСОВИМ ПРЕДСТАВЛЕННЯМ ІНФОРМАЦІЇ

Ю.В. Шабатура, к.т.н., доцент
Вінницький національний технічний університет
e-mail: shabatura@vstu.vinnica.ua

Сучасні засоби вимірювальної техніки в процесі свого функціонування здійснюють перетворення форми представлення вимірювальної інформації. Основні і найбільш важливі з метрологічної точки зору перетворення відбуваються в вимірювальних каналах. Енергія сигналу вимірюваної фізичної величини за допомогою вимірювального перетворювача перетворюється в енергію аналітичного сигналу, який забезпечує перенесення вимірювальної інформації про значення фізичної величини у формі своїх параметрів, або їх взаємного розташування. Наступне перетворення відбувається в процедурі вимірювання інформативних параметрів аналітичного сигналу. Причому результат останнього перетворення, як правило, має цифрову форму представлення, яку зручно обробляти у відповідних обчислювальних засобах, зберігати, передавати і т.п. Основною вимогою до розглянутих перетворень є забезпечення максимальної точності і надійності в отриманні вимірювальної інформації. З позицій даного критерію існуючі засоби „оцифровки" вимірювальної інформації за допомогою класичних АЦП рівня напруги інколи перестають задовольняти потреби споживачів. Тому розробка нових методів отримання інформації в цифровому вигляді про значення фізичних величин є актуальною для практики і важливою для науки.

Для вирішення означеної задачі пропонується нова структура перетворень вимірювальної інформації. Її суть полягає в попередньому перетворенні інформаційного сигналу про значення вимірюваної фізичної величини в еквівалентний часовий інтервал з наступним вимірюванням цього інтервалу, та відновленням результату в одиницях вимірюваної фізичної величини. Переваги запропонованого полягають в тому, що існуючі технічні засоби дозволяють вимірювати часові інтервали, представлені у вигляді тривалості імпульсів з роздільною здатністю до 30 двійкових розрядів включно (досягнута відносна похибка вимірювань не перевищує 10^{-15}). Крім того вимірювальні канали працюють в імпульсному режимі, це підвищує завадостійкість та зменшує енергоспоживання. Формально розглянуте перетворення є дискретним представленням аналогового сигналу $s(t) \in S(t)$ в межах інтервалу зміни поточного часу $t \in T$ у вигляді послідовності координат часової осі, $\{\Delta T_i, i = 0,1,2,...,N_k\}$ за значеннями яких можна отримати оцінку $\overset{*}{s}(t) \in \overset{*}{S}(t)$. Дискретне представлення аналогового вимірювального повідомлення у вигляді послідовності часових інтервалів і зворотнє до нього відновлення початкового повідомлення у вигляді оцінки $\overset{*}{s}(t)$ Можна записати в загальному вигляді $(\Delta T_0, \Delta T_1, \Delta T_2, ..., \Delta T_{N_k}) = \Im s(t); t \in T,$ $\overset{*}{s}(t) = \Re(\Delta T_0^*, \Delta T_1^*, \Delta T_2^*, ..., \Delta T_{N_k}^*); t \in T,$ де $\Im$ - оператор представлення, $\Re$ - оператор відновлення, ΔT_i^* - значення еквівалентних часових інтервалів за якими виконується відновлення початкового повідомлення, Т – інтервал поточного часу на якому здійснюється перетворення.

УДК 681.3:621.375

ВИСОКОЛІНІЙНІ ШВИДКОДІЮЧІ ПІДСИЛЮВАЧІ ПОСТІЙНОГО СТРУМУ ІЗ СИМЕТРИЧНОЮ СТРУКТУРОЮ

О.Д. Азаров д.т.н., професор,
В.А. Гарнага магістрант, С. В. Богомолов студент
Вінницький національний технічний університет
e-mail: azarov@vstu.vinnica.ua

Традиційно структури підсилювачів постійного струму містять у переважній більшості вхідні диференційні каскади та мають асиметричну структуру побудови, що призводить до таких наслідків асиметрія фронтів та нелінійність передатної характеристики.

Пропонується побудова підсилювальних схем за двотактною симетричною структурую відносно входу і виходу схеми. Симетрична структура передбачає наявність у підсилювачі двох каналів підсилення, побудованих на n-p-n та p-n-p транзисторах. Застосування такого підходу дає можливість отримати симетричну реакцію схеми на прямокутний двополярний вхідний імпульс, при цьому тривалості переднього і заднього фронтів вихідного сигналу майже однакові і підвищити лінійність переданої характеристики підсилювача, а також зменшити коефіцієнт нелінійних спотворень.

Усі підсилювачі, що пропонуються для розгляду автори поділили на такі групи:

1) із симетричною двотактною структурою та двотактними каскадоми на вході і на виході:
   а) середнім коефіцієнтом підсилення $10^3 \leq K_i \leq 10^4$;

б) високим коефіцієнтом підсилення. $10^4 \leq K_i \leq 10^6$

2) із симетричною структурою з диференційними каскадами на вході і двотактним каскадом по виходу та високим коефіцієнтом підсилення.

На рис. 1 представлено структуру двотактного симетричного підсилювача постійного струму з високим коефіцієнтом підсилення.

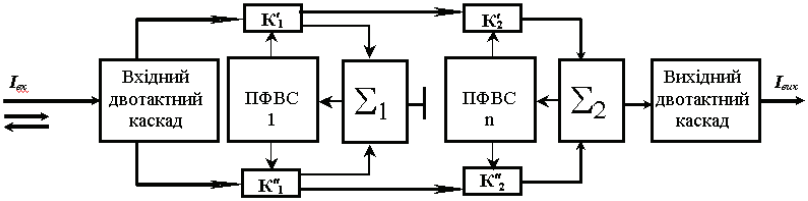


Рисунок 1 – Структура симетричного ППС із високим коефіцієнтом підсилення

Структура на рис. 1 містить двотакний вхідний каскад, два канали підсилення, кожен з яких складається з двох каскадів підсилення, два прафазних відбивача струму, та двотактний вихідний каскад.

Використання пропонованих структур дозволяє отримати такі переваги:

– більша швидкодія (вища частота зрізу АЧХ);
– симетричність форми вихідного сигналу при реакції на вхідний прямокутний двополярний імпульс;
– істотно менша нелінійність передатної характеристики;
– можуть працювати у “сплячому” режимі, при нульовому сигналі на вході схеми, що сприяє енергозбереженню в паузах між вхідними сигналами;
– менший коефіцієнт нелінійних спотворень у діапазоні частот.

УДК 681.32

КОРИГУВАННЯ ПОХИБОК КОМУТАТОРА ІВС ОПРАЦЮВАННЯ СТРИБКОПОДІБНИХ СИГНАЛІВ

А. В. Снігур, асистент
Вінницький національный технічний университет
e-mail: sanv12.mail.ru

Процес функціонування інформаційно-виімрювальних систем (ІВС) характеризується впливом різних зовнішніх факторів, зокрема температури, вологості тощо, що призводе до погіршення статичних характеристик їх вузлів, зокрема комутатора (К). У каналах сучасних ІВС опрацювання стрибкоподібних сигналів недостатньо враховується вплив факторів зовнішнього середовища, статичних похибок комутатора на кінцевий результат вимірювання параметрів досліджуваних сигналів, що може призвести до помилок у вимірюванні. Така ситуація обумовлює актуальність здійснення досліджень щодо коригування похибок комутатора.

Комутатор у складі ІВС характеризується статичними похибками проходження сигналів через закриті ключі. Метод, що пропонується для коригування похибок комутатора, передбачає подачу одразу на всі входи К однакової напруги $U_{вх.ком.}$, наприклад від додаткового ЦАП у складі каналу; спочатку розімкненим є перший ключ К (інші замкнені), потім – розімкненим є другий ключ і т. д. до n-го входу; при цьому отримується система рівнянь, що описує вихідну напругу $U_{вих.ком.i}$ (де і – номер входу, n – їх кількість) за умови однорідності структури К:

$$\begin{cases} U_{вих.ком.1} = U_{вх.ком.} + b_2 U_{вх.ком.} + b_3 U_{вх.ком.} + ... + b_n U_{вх.ком.}, \\ U_{вих.ком.2} = b_1 U_{вх.ком.} + U_{вх.ком.} + b_3 U_{вх.ком.} + ... + b_n U_{вх.ком.}, \\ U_{вих.ком.3} = b_1 U_{вх.ком.} + b_2 U_{вх.ком.} + U_{вх.ком.} + ... + b_n U_{вх.ком.}, \\ \vdots \\ U_{вих.ком.4} = b_1 U_{вх.ком.} + b_2 U_{вх.ком.} + b_3 U_{вх.ком.} + ... + U_{вх.ком.} \end{cases}$$

де b_i – похибки від неповного замикання і-го ключа. Вони можуть бути обчислені для всіх входів шляхом розв'язання системи з n рівнянь та n невідомих. При цьому значення $U_{вих.ком.i}$ є відомим і отримуються в АЦП (у складі ІВС), що кодує вихідну напругу К.

У загальному випадку b_i можуть визначатися для різних значень напруг (а для спрощення – усереднюватися для випадків подачі максимальної та мінімальної напруг діапазону із відповідними мінімальними та максимальними частотами): при подачі на входи постійної напруги, $U_{вх.ком.} = 0$, інших значень напруг із частотами, що лежить у межах вхідного діапазону, а також напруги $U_{вх} = U_{\max} \cdot \sin(w \cdot t)$ із максимальною амплітудою $U_{\max}$ та частотою w діапазону. На основі вказаної системи, результат комутації вхідних сигналів $U_{вх.ком.i}$ (де і – номер входу) для кожного з входів записується у вигляді

$$\begin{cases} U_{вх.ком.1} = U_{вих.ком.1} / (1 + b_2 + b_3 + ... + b_n), \\ U_{вх.ком.2} = U_{вих.ком.2} / (b_1 + 1 + b_3 + ... + b_n), \\ U_{вх.ком.3} = U_{вих.ком.3} / (b_1 + b_2 + 1 + ... + b_n), \\ \vdots \\ U_{вх.ком.n} = U_{вих.ком.n} / (b_1 + b_2 + b_3 + ... + 1). \end{cases} \qquad (1)$$

Базуючись на (1) можливо враховувати похибки К у обчислювальному пристрої каналу і таким чином зменшити його статичні похибки.

УДК 681.3:621.375

СХЕМА ПОРІВНЯННЯ З РЕГУЛЬОВАНОЮ ЧУТЛИВІСТЮ ДЛЯ ШВИДКОДІЮЧОГО ПОРОЗРЯДНОГО АЦП ІЗ ВАГОВОЮ НАДЛИШКОВІСТЮ

О.Д. Азаров, д.т.н., професор
О.О. Решетнік, магістрант
Вінницький національний технічний університет
e-mail: azarov@lili.vistu.vinnica.ua

Розглядаються методи побудови схем порівняння з регульованою чутливістю для швидкодіючих АЦП порозрядного врівноваження з ваговою надлишковістю. Використання компараторів струму з регульованою чутливістю дозволяє значно зменшити час перетворення. Це є можливим внаслідок компенсації динамічних похибок першого і другого роду за рахунок вагової надлишковості. Запропоновано в рамках структури схеми порівняння для побудови підсилювача різниці сигналів використовувати двотактну симетрійну структуру із введенням нелінійного зворотного зв`язку. Досліджено залежність між значенням різницевого сигналу і коефіцієнтом підсилення підсилювача різниці.

Для досягнення пропорційності між чутливістю схеми і часом встановлення доцільно використовувати для побудови схеми порівняння струмів підсилювача різниці із однополюсною АЧХ, яка є рівномірною у всьому діапазоні вихідного сигналу. Для досягнення максимальної швидкодії схеми порівняння струмів доцільно використовувати для побудови ПР двоканальний симетрійний ППС із нелінійним зворотнім зв`язком.

УДК 681.3

КОНДЕНСАТОРНІ ЦИФРОАНАЛОГОВІ ПЕРЕТВОРЮВАЧІ З ВАГОВОЮ НАДЛИШКОВІСТЮ

О.Д. Азаров, д.т.н., професор,
В.Г. Огнєв, студент
Вінницький національний технічний університет
e-mail: dadmin@list.ru

Конденсаторні цифроаналогові перетворювачі (ЦАП) з ваговою надлишковістю є складовою частиною швидкодіючих конденсаторних аналоговоцифрових перетворювачів (АЦП) із ваговою надлишковістю. Світовий досвід показує, що при використанні останніх можливо досягти гарних метрологічних показників даного класу пристроїв.

Цифроаналогові перетворювачі на конденсаторних матрицях працюють за рахунок перерозподілу заряду у вітках матриці. При подачі на вхід ЦАП цифрового сигналу відбувається підключення конденсатора кожної з віток ЦАП до джерела опорної напруги або заземлення. Таким чином утворюється конденсаторний дільник опорної напруги, який визначає вихідну напругу ЦАП.

Існує три класичних типи конденсаторних матриць ЦАП: ваговий, драбинковий, комбінований. (Рис 1. а, б, і в відповідно) Для кожного з них властиві свої співвідношення між номіналами конденсаторів.

Зв'язок між ємностями матриці вагового типу можна визначити за формулою $C_i = C\alpha^i$, де С – базовий номінал конденсатора, C_i - номінал *i*-го конденсатора матриці, α - основа системи числення ЦАП, i – номер розряду ЦАП,

який змінюється від 0 до *n-1*, *n* – кількість розрядів ЦАП. Номінал масштабного конденсатора C_∞ еквівалентний ємності матриці зі нескінченою довжиною ряду і визначається за виразом $C_m = C_\infty = C\dfrac{1}{\alpha - 1}$.

Для матриці драбинкового типу $C_i = C\alpha^0 = C$, $C_{зв} = C\dfrac{\alpha}{(\alpha-1)^2}$.

Для матриці комбінованого типу, якщо вона містить *m* конденсаторів на секцію, будуть характерними наступні співвідношення:

$C_i = C\alpha^{i-1}$, $C_{зв} = C\dfrac{\alpha^m}{(\alpha-1)(\alpha^m-1)}$, де $C_{зв}$ - номінал конденсатора зв'язку між секціями матриці.

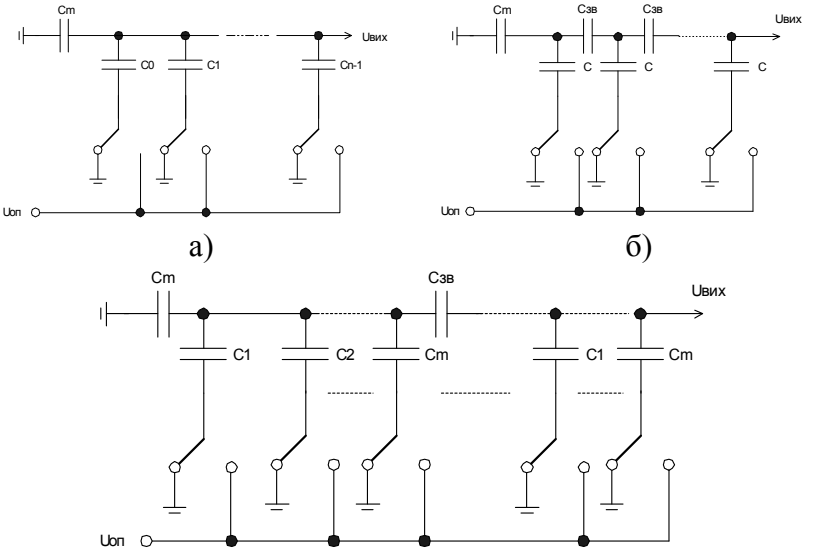


Рис. 1. Конденсаторні матриці а) – вагового типу; б) – драбинкового типу; в) – комбінованого типу

УДК 378

ВИРТУАЛЬНАЯ ЛАБОРАТОРИЯ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ КАК СРЕДСТВО ДИСТАНЦИОННОГО ОБУЧЕНИЯ

В.А. Романов, д.т.н., профессор
ИК НАН Украины, Киев, e-mail: dept230@insyg.kiev.ua
А.И. Крыжановский, зам. директора
Гуманитарно-педагогический колледж, Винница,
e-mail: neon69@ua.fm,
И.Б. Галелюка, м.н.с.
ИК НАН Украины, Киев, e-mail: dept230@insyg.kiev.ua

Современная социально-экономическая ситуация в стране и системе образования такая, что традиционные формы получения образования и модели обучения не могут удовлетворить потребности в образовательных услугах, обычно сконцентрированных в больших городах. Но как известно, никто не должен быть лишен возможности учиться через бедность, географические или временные изолированности, социальные незащищенности и невозможность посещать образовательные учреждения в силу физических недостатков или занятости производственными делами.

Выход состоит в поисках новых форм образования. Одной из них есть дистанционное обучение. Будучи следствием объективного процесса информатизации и вбирая в себя лучшие черты других форм образований, дистанционное обучение войдет в историю как наиболее перспективная, синтетическая, гуманистическая, интегральная форма образования.

Дистанционное обучение позволяет

конструировать учебный материал с учетом дифференциации творческой деятельности студентов, их возможностей и желания самостоятельно повышать свой профессиональный уровень, приводит к расширению педагогических методов и изменению характера учебного процесса. На современном этапе дистанционная форма обучения в Украине развивается в трех направлениях – сертификационное обучение, корпоративное обучение и обучение с целью получения определенного уровня образования.

Дистанционное обучение для современной системы высшего образования – это инновация, которая требует научных исследований и больших усилий для практической реализации и преодоления имеющихся педагогических, технологических и экономических проблем. Несмотря на отсутствие достаточной нормативно-правовой поддержки дистанционного обучения в высшей школе, многими отечественными коллективами ведутся активные работы в этой области.

Дальнейшее развитие дистанционного обучения в высшей школе требует формирования единой информационной образовательной среды. Для этого необходимо пойти по пути создания архивов общедоступных учебных материалов, которые базируются на унификации учебных компонентов.

В докладе будет проведен анализ существующих систем дистанционного образования, рассмотрены возможности их применения при подготовке младших специалистов и бакалавров в педагогических ВУЗах. Кроме того, будут оценены возможности построения систем дистанционного образования, которые используют в своей структуре технологии виртуальных лабораторий автоматизированного проектирования.

УДК 681.325; 681.335

ПІДВИЩЕННЯ ПАРАМЕТРИЧНОЇ НАДІЙНОСТІ АЦП ІЗ ВАГОВОЮ НАДЛИШКОВІСТЮ

О. Д. Азаров, д.т.н., професор,
О. В. Кадук, аспірант
Вінницький національний технічний університет

При оцінці надійності перетворювачів інформації (ПІ) необхідно враховувати можливість відмови його елементів, а також збої в роботі елементів цифрової частини. Це врахування грунтується на статистиці збоїв та відмов і використовує загальні методи оцінки надійності пристроїв. Відмови елементів ПІ можуть призводити або до повного виходу ПІ із ладу, або до появи похибки в результаті кодування.

Для врахування впливу на надійність кодування структури ПІ, алгоритму його роботи і значимість відмови пропонується використовувати два показники – ймовірність безвідмовної роботи, тобто відсутність відмов, що повністю виводять ПІ з ладу

$$p'(t) = e^{-\left(\sum_{j=1}^{k} \lambda_j\right) t},$$

де $\sum_{j=1}^{k} \lambda_j$ – сумарна інтенсивність відмов.

Інші відмови доцільно характеризувати величиною похибки, що ними вноситься. Такою оцінкою є математичне очікування похибки, обумовленої відмовами

$$M(\Delta) = \sum_{i=1}^{l} \Delta_i q_i ,$$

де q_i – ймовірність відмови i-го елемента, Δ_i – похибка, що ним вноситься.

Наукове видання

МЕТОДИ ТА ЗАСОБИ КОДУВАННЯ, ЗАХИСТУ Й УЩІЛЬНЕННЯ ІНФОРМАЦІЇ

Тези доповідей
першої Міжнародної науково-практичної конференції
м. Вінниця 15-17 травня 2007 року

Матеріали подаються в авторській редакції

Підписано до друку 27.04.2007
Гарнітура Times New Roman
Формат 29,7х42¼ Папір офсетний
Друк різографічний Ум. друк. арк. 8,1
Наклад 65 прим. Зам. № 2007-069

Віддруковано в комп'ютерному інформаційно-видавничому центрі Вінницького національного технічного університету
Свідоцтво Держкомінформу України
серія ДК №746 від 25.12.2001
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ,
гол. корпус, к. 114 тел. (0432) 59-81-59