Міністерство освіти і науки України
Вінницький національний технічний університет
Національний технічний університет України "КПІ"
Інститут кібернетики НАНУ
Південний Федеральний Університет (Росія)
Інститут інженерів з електротехніки та електроніки (IEEE), Українська секція

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

м. Вінниця, Україна
22-24 квітня 2009 року

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

г. Винница, Украина
22-24 апреля 2009 года

УНІВЕРСУМ-Вінниця
2009

УДК 681.32+621.391
М 54

Відповідальний редактор В.А. Лужецький

Матеріали статей опубліковані в авторській редакції

М 54 **Методи** та засоби кодування, захисту й ущільнення інформації. Тези доповідей другої Міжнародної науково-практичної конференції. м. Вінниця, 22-24 квітня 2009 року. – Вінниця: УНІВЕРСУМ-Вінниця, 2009. – 201 с.

ISBN 978-966-641-304-1

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

УДК 681.32+621.391

ISBN 978-966-641-304-1

ЗМІСТ

1. МЕТОДИ ТА ЗАСОБИ КОДУВАННЯ ІНФОРМАЦІЇ ТА ЦИФРОВОЇ МОДУЛЯЦІЇ

3. МЕТОДИ ТА ЗАСОБИ УЩІЛЬНЕННЯ ІНФОРМАЦІЇ

4. МЕТОДИ ТА ЗАСОБИ ПЕРЕТВОРЕННЯ ФОРМ ІНФОРМАЦІЇ

1. МЕТОДИ ТА ЗАСОБИ КОДУВАННЯ ІНФОРМАЦІЇ ТА ЦИФРОВОЇ МОДУЛЯЦІЇ

УДК 681.32.004; 681.518.5

КОД ХЕММІНГА-ФІБОНАЧЧІ, ЩО ВИПРАВЛЯЄ ПОМИЛКИ

І. В. Кузьмін[1], д.т.н., професор
О. В. Оводенко[2], к.т.н., доцент
І. В. Бугорська[3], магістр з інформаційної безпеки
[1]Вінницький національний технічний університет
[2]Донецький національний технічний університет
[3]Вінниця, Україна
ovodenko@km.ru

Відомо кілька різновидів коду Хеммінга, які мають різну здатність щодо виявлення і виправлення помилок. Метод їх побудови однаковий і передбачає використання звичайного ненадлишкового двійкового коду як первинного коду. Крім того, результат контрольних перевірок також є ненадлишковим двійковим кодом.

У доповіді розглядається підхід до побудови модифікованого коду Хеммінга, який базується на використанні як первинного коду надлишкового коду Фібоначчі і використанні надлишкової кількості контрольних перевірок, результат яких також є кодом Фібоначчі.

(n,k)-код Хеммінга-Фібоначчі містить k інформаційних і $r = n - k$ контрольних символів, кількість яких визначається із співвідношення:

$$r \geq \varphi(r+1) - k - 1,$$

де $\varphi(r+1)$ - $(r+1)$-е число Фібоначчі.

У загальному випадку контрольні символи розташовуються на позиціях з номерами $\varphi(i)$, а на інших позиціях – інформаційні символи за їх порядком у первинному коді.

Контрольна перевірка з номером i виконується для розрядів коду Хеммінга-Фібоначчі, номери яких містять символ 1 у i-му розряді їх представлення у вигляді коду Фібоначчі.

Код Хеммінга-Фібоначчі у 1,5 рази довше звичайного коду Хеммінга і забезпечує виправлення не тільки однократних, а й двократних помилок. Крім того, забезпечується виявлення значної частини багатократних помилок.

Наводиться приклад побудови (12,7)-коду, який має таку структуру:

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}
k_1	k_2	k_3	a_1	k_4	a_2	a_3	k_5	a_4	a_5	a_6	a_7

де $x_l\left(l=1,2,...,12\right)$- розряди коду;

$k_i\left(i=1,2,...,5\right)$- контрольні символи;

$a_j\left(j=1,2,...,7\right)$- інформаційні символи.

Контрольні перевірки описуються виразами:

$s_1 = x_1 \oplus x_4 \oplus x_6 \Rightarrow x_1 \oplus \left(x_4 \vee x_6\right)$;

$s_2 = x_2 \oplus x_7$; $s_3 = x_3 \oplus x_4$;

$s_4 = x_5 \oplus x_6 \oplus x_7 \Rightarrow x_5 \oplus \left(x_6 \vee x_7\right)$;

$s_5 = x_8 \oplus x_9 \oplus x_{10} \oplus x_{11} \oplus x_{12} \Rightarrow x_8 \oplus \left(x_9 \vee x_{10}\right) \oplus \left(x_{11} \vee x_{12}\right)$,

а контрольні символи визначаються за формулами:

$k_1 = a_1 \oplus a_2 \Rightarrow a_1 \vee a_2$;

$k_2 = a_3$; $k_3 = a_1$;

$k_4 = a_2 \oplus a_3 \Rightarrow a_2 \vee a_3$;

$k_5 = a_4 \oplus a_5 \oplus a_6 \oplus a_7 \Rightarrow \left(a_4 \vee a_5\right) \oplus a_6 \vee a_7$.

Тут після стрілок показано спрощені вирази, які випливають з того, що у М-формі коду Фібоначчі поруч не може бути дві одиниці. Це забезпечує спрощення апаратної реалізації кодера-декодера коду Хеммінга-Фібоначчі, порівняно з кодером-декодером звичайного коду Хеммінга.

УДК 621.394.147

ВИЗНАЧЕННЯ ВЛАСТИВОСТЕЙ ОСНОВНИХ КОДОВИХ СИСТЕМ ГАЛУА

Л.Б. Петришин (L. Petryshyn)[1], д.т.н., професор
М.В. Лаврів[2], асистент
[1]Гірничо-металургійна академія м. Краків, Польща
(AGH University of Science and Technology Krakow, Poland)
[2]Прикарпатський національний університет
[1]petryshynl@poczta.fm, petryshynl@mail.ru
[2]dlyamarii@gmail.com

Коди полів Галуа класифікують як блокові поліномні циклічні коди. При кодуванні повідомлення ототожнюються з поліномами, а сама процедура кодування полягає в їх перемноженні на фіксований поліном. Для блокових (n,m) - кодів в кожному блоку визначаються $l = m - n$ контрольних символів. В масиві поля $GF(2^n)$ повна кодуюча матриця має розмірність $N \times N$ ($N=2^n$), в якій кодуючими векторами є поліноми розмірності n, впорядковані в матрицю $N \times n$, а решта $N - n$ розрядів носять характер надлишковості для завадозахисту, а їхня кількість l визначає степінь захисту та кількість потенційно корегованих помилок.

Елементарним є просте, або *рекурсивне* впорядкування кодових елементів в породжуючій матриці, яке відображається із системи функцій Галуа з рекурсивним впорядкуванням. В матриці $Gl(2^n)$ розмірності $N \times N$ виділять власне матрицю рекурсивної кодової системи Галуа $N \times n$ з паралельним впорядкуванням кодових елементів та матрицю-стовпець розмірності $N \times l$ з вертикальним векторним впорядкуванням. На основі рекурсивної кодової системи реалізовані ефективні засоби системних функцій

вертикальної інфотехнології, що дозволяють реалізувати наступні переваги перед існуючими число-імпульсними системами: - маршрутизацію повідомлень із розподіленим доступом до джерел повідомлень ієрархічно від диспетчера мережі до джерел повідомлень; - вибір даних про поточний стан джерела повідомлень в довільний момент часу за n останніми зареєстрованими символами коду Галуа; - самокорекцію прийнятого спотвореного коду за l надлишковими зчитаними символами; - скорочення часу ідентифікації інтегрального стану кодованого джерела до $T = n\,\tau$, де τ - усереднений параметр активності джерела інформації на періоді слідування n останніх аналізованих символів Галуа; - зменшення об'ємів повідомлень, що обробляються. Проте, рекурсивній кодовій системі властивий значний час ідентифікації стану джерел повідомлень із низькою активністю.

Вперше розроблена та досліджена *кодонна* кодова система Галуа, в значній мірі позбавлена вказаного недоліку. Поле, яке генерується кодонним методом, породжується послідовністю Галуа, вектор-кодони якої утворюють байторієнтоване тривимірне упорядкування витків абстрактної повної спіралі n-розрядних $N - 1$ кілець Галуа, замкнутих послідовно між собою в тор з циклом $M = n\,(N–1) = n\,(2^n–1)$. Внаслідок того, що кодонна кодова система Галуа потребує паралельного подання кожного із повідомлень n-розрядними словами, в полі $N \times N$ виділяється кодова матриця розмірності $N \times n$. Відповідно кожному інформаційному імпульсу ставиться у відповідність n-розрядний вектор-кодон, який однозначно визначає інтегральний стан джерела повідомлень. Ефективність методу визначається простотою реалізації кодуючого пристрою на регістрі зсуву із зворотними зв'язками при тактуванні вихідного вектора a пачками із n імпульсів. Час ідентифікації інтегральної характеристики зменшується до періоду τ слідування інформаційних

повідомлень, який додатково визначає поточну активність джерела повідомлень. Проте висуваються більш жорсткі вимоги щодо пропускної здатності каналів зв'язку.

При мікроміниатюризації перетворювачів лінійних та кутових переміщень на основі кодових шкал виникають технологічні труднощі виготовлення зчитувачів. Рознесення зчитувачів через постійну кількість кодових елементів дозволяє спростити технологічні проблеми, але вимагає впровадження нової матриці теоретико-числових перетворень із розрідженим впорядкуванням кодових векторів. Вперше розроблена та досліджена кодова система Галуа з дискретним розрідженням кодових послідовностей, на основі якої розроблений ряд високоефективних перетворювачів форми інформації. Базою розрідженої кодової системи Галуа є розріджене впорядкування функцій Галуа, на основі якого синтезовано породжуючу матрицю кодової системи. Так як дане впорядкування передбачає паралельне векторне пакування кодових елементів із наскрізною рекурсією, матриця розмірності $N \times n$ формується шляхом вибіркового групування через визначений крок розрідження суміжних кодових елементів вихідної кодової матриці. Поле Галуа, породжене наведеним методом, володіє основними властивостями кодонної моделі при ноніусному зчитуванні та властивостями рекурсивної моделі - при звичайному.

Використовуючи математичний апарат кодування в полях Галуа, реальним є вибір кодової системи, що найкращим чином реалізує технічні вимоги до перетворювачів форми інформації та враховує структуру сигналу перетворення.

УДК 621.3.037.37

ЗАВАДОСТІЙКА ПЕРЕДАЧА ДАНИХ НА БАЗІ ФАКТОРІАЛЬНИХ ЧИСЕЛ

О. А. Борисенко, д.т.н., професор
О. Є. Горячев, аспірант
Сумський державний університет
electron@sumdu.edu.ua

Вступ

Кодування даних у вигляді факторіальних чисел дає можливість виявляти та виправляти деякі помилки в даних, які передаються по каналах зв'язку. Крім того, факторіальні системи числення можуть бути застосовані для побудови перестановок. Перестановки, з урахуванням розташування і значень їх елементів, також можуть бути застосовані для виявлення та корекції помилок.

Загальні положення

Факторіальні системи числення належать до систем зі змішаною основою. Зазвичай під факторіальною системою числення розуміють вираз, який має вигляд:

$$F_{<ф>} = X_n \cdot n! + X_{n-1} \cdot (n-1)! + \ldots + X_l \cdot l! + \ldots + X_1 \cdot 1! + X_0 \cdot 0!,$$

де $l = 0,1,\ldots,n$; $0 \le X_l \le l$.

Цей вираз має назву нумераційної функції. Максимальне число у факторіальній системі має вигляд

$$F_{<\text{ф}>\max} = (n+1)! - 1.$$

Мінімальне число $00...0...0$ у факторіальній системі числення $F_{\min} = 0$.

Діапазон факторіальних чисел

$$P = F_{\max} + 1.$$

Перетворення факторіальних чисел в однорідні числа

Перетворення факторіального числа в однорідне виконується шляхом підстановки факторіального числа в числову (нумераційну) функцію для факторіальних систем числення. При цьому виконуються всі вказані в цій функції операції множення і додавання.

Перетворення однорідних чисел у факторіальні

Першим кроком перетворення числа із однорідної системи числення у факторіальну є ділення числа, що перетворюється, на 1. Залишок у цьому випадку буде створювати цифру нульового розряду. На кожному наступному кроці перетворення відбувається ділення залишку, отриманого при діленні на попередньому кроці на число, на 1 більше за дільник попереднього кроку, тобто відбувається послідовне ділення на 1, 2 3 і т.д. При цьому на кожному кроці аналізується величина отриманої частки. Якщо вона менше за наступний дільник, то в старший розряд факторіального числа записується її значення, а якщо дорівнює або більша за нього, то виконується наступний крок ділення, яке продовжується до того часу, поки частка не стане менша за свого дільника. Потім ця частка виписується і справа наліво за нею виписуються всі отримані раніше залишки. Їх послідовність створює факторіальне число, яке потрібно було знайти.

Виявлення помилок

При передачі даних у вигляді факторіальних чисел по каналу зв'язку з перешкодами можуть бути одержані помилкові числа. Ознакою помилок буде порушення обмежень щодо величини цифр X_l, де $0 \le X_l \le l$.

Наприклад, факторіальне число 23210 є правильним, а число 23220 – помилковим, оскільки в першому розряді цього числа порушене обмеження щодо величини його цифри, яка повинна бути не більшою за 1, тобто дорівнювати 0 або 1.

УДК 512.728.2

ПРЕОБРАЗОВАНИЕ ДВОИЧНЫХ КОДОВ В УНИТАРНЫЕ БИНОМИАЛЬНЫЕ И ОБРАТНО

А. А. Борисенко, д.т.н., профессор
В. В. Петров, аспирант
Сумской государственный университет
electron@sumdu.edu.ua

На практике перспективным является применение биномиальных счетных схем, построенных на основе унитарной биномиальной системы счисления. Эти схемы обладают повышенным быстродействием и содержат природную избыточность, которую можно использовать для повышения помехоустойчивости. Поскольку двоичные коды нашли широкое применение на практике, актуальным является разработка эффективных методов перевода унитарных биномиальных чисел в двоичные и обратно.

Одним из универсальных методов перевода числа для любых систем счисления заключается том, что операция перевода представляется в виде двух параллельных процедур счета – сложения и вычитания. В процессе преобразования от переводимого числа последовательно отнимаются единицы с единовременным прибавлением единиц ко второму числу. При этом первым является переводимое число, а вторым – ноль. Процедуры вычитания и добавления единиц производятся по правилам выполнения этих операций в системах счисления, в которых находятся каждое из чисел. Процесс счета заканчивается, когда переводимое число станет равным нулю, при этом второе число будет эквивалентно исходному первому. В общем виде структурная схема преобразователя, использующего последовательный

перебор чисел, для перевода из одной системы счисления в другую приведена на рис. 1

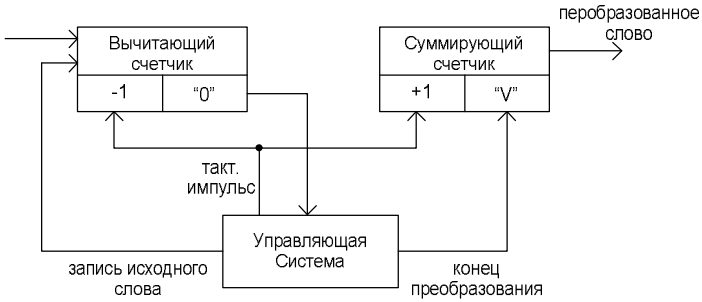


Рис. 1 – Структурная схема преобразователя чисел

В случае преобразования двоичного кода в унитарный биномиальный, вычитающий счетчик будет двоичным, а суммирующий – унитарным биномиальным, при боратном переходе – от биномиального к двоичному счетчики меняются местами. Рассмотрим преобразование двоичного числа в унитарное биномиальное. В исходном состоянии оба счетчика находятся в нуле. После занесения переводимого двоичного числа в вычитающий счетчик схема управления начинает процесс преобразования. Преобразование длится до тех пор, пока вычитающий счетчик не перейдет в нулевое состояние. В этот момент в суммирующем счетчике будет находиться число эквивалентное первому. После этого процесс преобразования будет завершен. Результат снимается с выхода суммирующего унитарного биномиального счетчика, и управляющая система переведет оба счетчика в исходное нулевое состояние. По занесению очередного двоичного числа процесс преобразования повторяется сначала.

УДК 519.728.2

ОЦЕНКА ПОМЕХОУСТОЙЧИВОСТИ РАВНОВЕСНЫХ КОДОВ 1 ИЗ N

А. А. Борисенко, д.т.н., профессор
Д. В. Гутенко, аспирант; В. В. Кремезный, студент
Сумський Государственный университет
electron@sumdu.edu.ua

На практике широко используются равновесные коды, в частности их разновидность коды 1 из N. В этом коде работают дешифраторы и распределители импульсов. Эти коды обладают естественной избыточностью и соответственно помехоустойчивостью. При этом возникает задача оценить их помехоустойчивость.

В равновесном коде 1 из N при передаче сигнала через канал связи, любая N-разрядная правильная комбинация может перейти в любую другую из 2^N возможных комбинаций, среди которых будет 2^N-N обнаруживаемых ошибочных комбинаций. Кроме обнаруживаемых ошибочных комбинаций существуют необнаруживаемые ошибочные комбинации, когда происходит переход правильной комбинации в любую другую комбинацию с одной единицей. Количество необнаруживаемых ошибочных комбинаций равно N-1, так как учитывается, что среди 2^N комбинаций одна будет правильной. Тогда сумма всех обнаруживаемых и необнаруживаемых ошибочных комбинаций, а также правильной комбинации будет равна 2^N, так как 2^N-N+ +(N-1)+1=2^N. Число таких комбинаций равно числу переходов правильной комбинации в любую другую.

Максимальная доля обнаруживаемых ошибочных переходов будет равна $D = 1 - (N / 2^N)$.

Правильной передаче, чему соответствует переход комбинации в саму себя, то есть единица должна перейти в единицу, а во всех остальных разрядах нули должны перейти в нули. Для исходной комбинации вероятность правильного перехода равна $П = (P_{00})^{N-1} P_{11}$.

При необнаруживаемом ошибочном переходе одна разрешенная комбинация должна перейти в другую разрешённую, то есть в комбинацию с одной единицей и N-1 нулями. Это возможно если единичный разряд перейдёт в нулевой, а один нулевой перейдёт в единицу. Все остальные N-2 нуля должны перейти в нули. Соответственно вероятность перехода правильной комбинации в любую другую разрешённую комбинацию. $V = (N-1)(P_{00})^{N-2} P_{10} P_{01}$.

Следовательно, вероятность перехода правильной комбинации в любую запрещённую комбинацию равна $Z = 1-(N-1)(P_{00})^{N-2} P_{10} P_{01} - (P_{00})^{N-1} P_{11}$.

Для определения среднего значения вероятностей переходов правильных комбинаций в необнаруживаемые ошибочные и в саму себя необходимо учитывать вероятности появления той или иной исходной комбинации. Однако было доказано, что для любых равновесных кодов вероятностные величины, которые характеризуют одну комбинацию равновесного кода, могут применяться для средней величины, характеризующей весь код. Поэтому вероятности V и П для одной комбинации являются также средними значениями вероятностей переходов правильных комбинаций в необнаруживаемые ошибочные и в саму себя. Определив значения вероятностей и других характеристик из вышеприведенных формул, можно узнать, насколько помехоустойчивым является тот или иной код 1 из N.

УДК 621.37:621.391

ПОЛІНОМІАЛЬНИЙ МЕТОД ПЕРЕВІРКИ СКЛАДНИХ СТАТИСТИЧНИХ ГІПОТЕЗ

В. В. Палагін[1], к.т.н., доцент
О. А. Палагіна, к.т.н., доцент
Черкаський державний технологічний університет
[1]palahin@yahoo.com

Задача розпізнавання сигналів на тлі завад є однією з важливих та актуальних в багатьох прикладних галузях, зокрема в телекомунікаційних системах, радіолокації, технічній діагностиці тощо, де, враховуючи випадковий характер сигналів, розглядають статистичну інтерпретацію проблеми розпізнавання на рівні перевірки складних статистичних гіпотез (критерій Байеса, Неймана-Пірсона).

Аналізуючи стан наукових досліджень в даному напрямку можна сказати, що актуальними залишаються питання розробки та вдосконалення математичного апарату для розв'язання таких задач, де розглядається розпізнавання сигналів на тлі негауссівських завад, як найбільш узагальнених моделей завад.

Метою роботи є побудова та дослідження поліноміальних нелінійних ефективних алгоритмів розпізнавання сигналів, що приймаються на тлі негауссівських завад, застосовуючи адаптований асимптотично нормальний моментний критерій якості (Yu).

Нехай на вході системи спостерігається випадковий сигнал $\xi_i(t)$, $i = \overline{1, N}$ у вигляді адитивної суміші корисного сигналу $s_i(t)$ і завади $\eta(t)$, яка розподілена за негауссівським законом з нульовим математичним сподіванням та представляється у вигляді моментно-кумулянтного опису.

По результатам обробки випадкового сигналу $\xi_i(t)$ необхідно винести рішення про виконання однієї з гіпотез H_i, коли спостерігається вибірка корисного сигналу виду $\xi_{iv} = s_{iv}(\alpha_k) + \eta_v(\gamma_k)$, чи гіпотези H_0, коли приймається лише завада – $\xi_{0v} = \eta_v(\gamma_k)$, де $s_{iv}(\alpha_k)$ – сигнал з відомими параметрами α_k; $\eta_v(\gamma_k)$– негауссівський випадковий процес з відомими кумулянтами γ_k, $k = \overline{0,n}$. Таким чином постає задача розпізнавання – виявлення сигналу та віднесення його до відповідного класу, що відповідає номеру гіпотези H_i.

Показано, що для рішення поставленої задачі щодо перевірки гіпотез H_m і H_r, можна використовувати узагальнене вирішальне правило (ВП) виду

$$\Lambda_{mr}(\vec{x})_{sn} = \sum_{i=1}^{s}\sum_{v=1}^{n} k_{iv}^{(mr)} x_v^i + k_0^{(mr)} \underset{H_m}{\overset{H_r}{\gtrless}} 0 \quad , r, m = \overline{1, N}\,,\ r \neq m\,,$$

де оптимальні коефіцієнти даного ВП, які мінімізують ймовірності помилок першого та другого роду, знаходяться згідно Yu:

$$Yu(T,G)_{(mr)} = \left[\left(G_{mr}^{(m)}\right)^{0,5} + \left(G_{mr}^{(r)}\right)^{0,5}\right]^2 \left[T_{mr}^{(m)} - T_{mr}^{(r)}\right]^{-2},$$

де $T_{mr}^{(m)}$, $T_{mr}^{(r)}$, $G_{mr}^{(m)}$, $G_{mr}^{(r)}$ - математичне сподівання та дисперсії ВП при гіпотезах m та r.

Використовуючи даний підхід, синтезовані нелінійні ВП, які дозволяють враховувати тонку структуру негауссівських завад у вигляді кумулянтних коефіцієнтів асиметрії, ексцесу тощо, що в цілому призводить до зменшення ймовірностей помилок першого та другого роду ВП в порівнянні з добре відомими результатами, отриманими за класичними імовірнісними критеріями якості.

УДК 621.396.2:681.327.8

МОДЕЛЬ ОПТИМАЛЬНОГО МАНЧЕСТЕРСЬКОГО КОДУ ВОЛОКОННО-ОПТИЧНИХ СИСТЕМ ПЕРЕДАЧІ ІНФОРМАЦІЇ

В. М. Лисогор[1], д.т.н., професор
Г. Л. Лисенко[2], к.т.н., доцент
С. В. Шуллє[2], пошукач
Вінницький державний аграрний університет
Вінницький національний технічний університет
[2]S_Shulle@ukr.net

Основні параметри будь-якої волоконно-оптичної системи передачі інформації (довжина ділянки, стійкість синхронізації, перешкодозахисна та ін.) в значній мірі залежать від вибору коду в лінії (лінійного коду).

Особливості побудови лінійних кодів залежать від фізичних властивостей середовища розповсюдження сигналів і кінцевих пристроїв. Оптичне волокно, а також джерело інформаційних повідомлень, фотоприймач пред'являють специфічні вимоги до параметрів сигналу, що передається з їх допомогою. Це визначається тим, що імпульсні сигнали оптичної потужності, що випромінюються, можуть бути тільки позитивними або нульовими, що робить неможливим безпосереднє використання біполярних кодів, як це здійснюється в класичній електроніці і використанні в системах зв'язку по електричному кабелю.

Іншою проблемою, що виникає при передачі по лініях волоконно-оптичного зв'язку цифрових сигналів, є необхідність забезпечення побітової синхронної роботи передавача і приймача (тактова синхронізація).

Дальність зв'язку без додаткового приймання

волоконно-оптичних інтерфейсів більшості мережевих стандартів досягає 2 км. При такій великій відстані між приймачем та передавачем прокладка окремої лінії для передачі синхросигналів технічно і економічно недоцільна, тому більш вигіднім є механізм внутрішнього частотного підстроювання в безпосередньому лінійному сигналі. Для реалізації цього механізму застосуємо коди, що самосинхронізуються. Ідея такого кодування полягає в тому, щоб на фізичному рівні моделі OSI змінити початкову послідовність інформації, що передається додаванням нових символів таким чином, щоб в лінійному сигналі містилася інформація про тактову частоту початкової імпульсної послідовності.

В широко поширених системах FDDI (Fiber Distributed Data Interface – розподілений волоконно-оптичний інтерфейс) і Fast Ethernet використовується блоковий код 4B5B, в якому чотири біти початкового повідомлення представляються в лінії п’ятьма бітами. При передачі символів даних щонайменше один з п’яти бітів відмінний від інших. Використання блокового кодування типу 4B5B дозволяє збільшити швидкість передачі в лінії всього на 25%, коли вона складає 125 Мбіт/с замість 200 Мбіт/с, необхідних для манчестерського кодування.

Досліджено і вдосконалено модель оптимального лінійного кодування в волоконно-оптичних систем передачі інформації і розподілених оптичних мережах, як сукупності технічних засобів передачі інформації від об’єктів до адресатів на основі використання оптоволоконних ліній зв’язку для створення середовища розповсюдження сигналів.

УДК 681.3:519.62

ПЕРЕДАЧА ЦИФРОВОЙ ИНФОРМАЦИИ НА ОСНОВЕ МАНИПУЛЯЦИИ ПАРАМЕТРАМИ ФУНКЦИИ ПЛОТНОСТИ ВЕРОЯТНОСТИ СЛУЧАЙНОГО ПРОЦЕССА

С. Б. Приходько, к.т.н., доцент
Национальный университет кораблестроения
sbp@ustu.edu.ua

В последнее время для улучшения помехоустойчивости систем цифровой связи и защиты передаваемой информации предпринимаются попытки использования негармонических несущих сигналов и новых видов манипуляции. Одной из таковых является манипуляция случайного процесса (stochastic process shift keying, SPSK) – метод кодирования цифровой информации, при котором на заданном временном интервале один случайный процесс представляет нулевое значение бита, а другой – единичное значение. Для реализации SPSK известны подходы, основанные на применении уравнений авторегрессии/скользящего среднего (АСС), стохастических дифференциальных уравнений (СДУ), симметричных нелинейных преобразований (СНП) коэффициента эксцесса и асимметрии случайного процесса. Заметим, применение СНП дает возможность сохранять дисперсию постоянной для всех несущих информацию случайных процессов, что повышает защиту передаваемой информации. С другой стороны, в отличие от СНП использование АСС и СДУ позволяет задействовать большее число параметров, через которые в несущий случайный сигнал вводится информация, что увеличивает скорость ее передачи. Возникает вопрос:

нельзя ли объединить отмеченные положительные качества в каком-то одном подходе? Оказывается это возможно. Цель данной работы состоит в том, чтобы показать эту возможность и предложить соответствующий подход для ее реализации.

В работе предлагается подход, основанный на применении нелинейных СДУ, в состав каждого их которых входят параметры функции плотности вероятности (ФПВ) соответствующего случайного процесса, моделируемого этим СДУ. Построение указанных СДУ осуществляется предложенным ранее автором методом структурной идентификации на основе применения математических моделей (СДУ) нормализованных случайных сигналов. Для примера построения искомого СДУ в работе используется преобразование Джонсона для семейства распределений S_U и СДУ нормализованного случайного процесса $z(t)$

$$\dot{z} + \alpha_z z = \sqrt{2D_z\alpha_z}\, n(t), \qquad (1)$$

где $n(t)$ – белый шум.

Для S_U преобразование Джонсона имеет вид

$$z = \gamma + \eta h(x,\varphi,\lambda),\ h(x,\varphi,\lambda) = Arsh(\bar{x}), \qquad (2)$$

где γ, η, λ, φ – параметры ФПВ Джонсона случайного процесса $x(t)$; $\bar{x} = (x-\varphi)/\lambda$; $Arsh(\bar{x}) = \ln\left[\bar{x} + \sqrt{\bar{x}^2+1}\right]$.

СДУ для $x(t)$ определяется на основе (1) и (2)

$$\dot{x} + \lambda\alpha_z\left[\gamma/\eta + Arsh(\bar{x})\right]\sqrt{\bar{x}^2+1} - \lambda D_z\alpha_z\bar{x}/\eta^2 =$$
$$= \lambda\sqrt{2D_z\alpha_z[\bar{x}^2+1]}\,n(t)/\eta\,.$$

Информация вводилась через параметры γ и η. Результаты компьютерного моделирования показали работоспособность предложенного подхода.

УДК 681.32

МЕТОД ПРОВЕРКИ ИСКАЖЕННОГО СЛОВА КОДА ГОППЫ

В. Е. Федюкович
ГлобалЛоджик, г.Киев
vf@unity.net

Рассматривается задача проверки утверждения об искаженном кодовом слове кода Гоппы. Изучается метод проверки утверждений, предоставляющий проверяющей стороне минимально необходимую информацию, а также исключающий возможность для проверяющей стороны распространять достоверную информацию о справедливости проверяемого утверждения.

Проверяется утверждение об ошибке в искаженном кодовом слове, положительное решение принимается если вес ошибки (метрика Хэмминга) не превышает заданный порог. Проверяющей стороне доступно искаженное кодовое слово, порог, а также экземпляры привязки (commitment) к кодовому слову и к коэффициентам полинома Гоппы. Используется схема привязки Pedersen'а для элемента конечного поля. Доказывающей стороне доступно кодовое слово и полином Гоппы в явном виде.

Предложен новый протокол аргумента знания с нулевым разглашением в модели с честным Проверяющим (honest Verifier zero knowledge argument of knowledge) кодового слова и полинома Гоппы, а также проверки справедливости утверждения об ограниченной ошибке. Протокол использует разработанную автором схему запрос-ответ, предназначенную для проверки утверждений о корнях уравнений над конечным полем и над кольцом целых чисел. В рамках схемы запрос-ответ строится

проверочный полином, в котором недоступные для проверки значения заменяются ответами протокола Шнорра. Свойство корректности протоколов, использующих эту схему, опирается на утверждение о количестве корней уравнения (лемма Швартца-Зиппеля).

Предложенный протокол может использоваться как элемент схемы водяных знаков (watermark) с публичной информацией, устойчивой к некоторому уровню искажений.

Также были получены протоколы аргумента знания, предназначенные для проверки утверждений о множествах, графах (изоморфизм, раскраска вершин в 3 цвета, существование цикла Гамильтона), строках.

УДК 612.766

ОБРОБКА ПУЛЬСОВОГО СИГНАЛУ ДЛЯ ПОЗБАВЛЕННЯ ЙОГО ШУМОВИХ КОМПОНЕНТ

В. В. Гніліцький[1], к.т.н., доцент
Н. В. Мужицька[2], асистент
Житомирський державний технологічний університет
[1]gnil@ztu.edu.ua, [2]muzitskaya_zh@rambler.ru

Показники пульсу здавна застосовують для оцінки стану серцево-судинної системи, а також інших органів і систем організму людини.

Встановлено закономірності, що визначають різноманіття форм пульсових сигналів, зареєстрованих з різних органів людини в умовах нормальних, патологічних і стресових ситуацій. На підставі цього розроблено безліч методів діагностики.

Для здійснення комплексної оцінки стану судин та діагностики хвороб, викликаних змінами в роботі судинних стінок, найчастіше вимірюють параметри пульсової хвилі.

Вейвлет-аналіз – це сучасний та перспективний метод обробки даних. Методи вейвлет-аналізу можна застосувати до даних різноманітної природи. Це можуть бути, наприклад, одновимірні функції чи двовимірні зображення.

Для того, щоб з'ясувати наскільки ефективно працює вейвлет-аналіз по виділенню шуму з пульсового сигналу, до модельних даних додамо шум з нормальним законом розподілу, з амплітудами шуму рівними 1-10% амплітуди корисного сигналу.

Застосуємо до всіх зашумлених сигналів процедуру дискретного вейвлет-перетворення і проаналізуємо, яким чином можна відновити сигнали в процедурі зворотного

перетворення так, щоб позбутися шумів та зайвих компонент. У процесі розкладу аналізованого сигналу на два рівні було виділено три компоненти, причому за візуальним аналізом можна стверджувати, що два молодших рівні розкладу представляють шумову компоненту, ймовірно – гаусовий шум. А третя компонента являє собою знешумлений модельний сигнал.

Тепер проаналізуємо більш детально, за яким принципом слід проводити процедуру синтезу сигналу за набором вейвлет-коефіцієнтів у випадку, коли слід позбавитись від шуму. Проведемо процедуру розкладу на різних рівнях і з'ясуємо, яку похибку при відтворенні сигналу ми отримаємо при різних варіантах синтезу.

Спираючись на отримані результати, проведемо процедуру дискретного вейвлет-аналізу для сигналів з різним рівнем шуму. Аналіз реалізуємо різними методами та для різної кількості дискретних рівнів розкладу.

Візуальний аналіз отриманих нами даних чітко свідчить, що для позбавлення від шуму при розкладі вибраними вейвлетами в процедуру відновлення сигналу слід включати всі рівні розкладу, окрім двох молодших. Щоб підтвердити цю гіпотезу чисельними показниками, після того, як ми отримали знешумлені сигнали за описаною методикою для всіх варіантів розкладу, нами були розраховані відповідні коефіцієнти кореляції.

Залежність коефіцієнтів кореляції від рівня шуму співпадає для всіх рівнів розкладу вейвлета Добеші, це ще раз підтверджує сформульоване нами правило синтезу сигналу за результатами вейвлет-розкладу.

УДК 681.32

МЕТОД ВЫЧИСЛЕНИЯ БИНОМИАЛЬНЫХ КОЭФФИЦИЕНТОВ НА ОСНОВЕ ДВОИЧНО-КАНОНИЧЕСКОЙ ФОРМЫ ЗАПИСИ ЧИСЕЛ

И. А. Кулик, к.т.н., доцент; Е. М. Скордина, студент
Сумский государственный университет
fair.sumy@mail.ru

Часто в практике нумерационного кодирования возникает необходимость оперировать большими числами, например числами сочетаний C_n^k при больших значениях n и k, где n – длина кодируемых двоичных последовательностей, а k – количество содержащихся в них единиц. Но хранение и оперирование огромными числами C_n^k (например, $C_{1000}^{300} \approx 5,42 \times 10^{263}$), связано с необходимостью использования большого количества двоичных разрядов. Следовательно, актуальной является разработка метода представления чисел C_n^k при больших параметрах n и k. В связи с этим предлагается к рассмотрению двоично-каноническая форма записи числа, основанная на разложении его на простые числа:

$$z = q_1^{a_1} q_2^{a_2} \ldots q_j^{a_j} \ldots q_m^{a_m},$$

где q_j – j-й элемент ряда простых чисел, $j = 1, 2, \ldots, m$;

a_j – показатель степени простого числа q_j;

m – количество простых чисел q_j, необходимых для представления числа z.

Согласно канонической форме записи произведения и деления чисел для подсчёта C_n^k могут быть заменены операциями суммирования и вычитания над степенями

простых чисел, составляющих их, как показано в выражении:

$$C_n^k = \frac{n!}{k!(n-k)!} = \frac{q_1^{a_1} \cdot q_2^{a_2} \cdot \ldots \cdot q_m^{a_m}}{(q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_m^{b_m}) \cdot (q_1^{c_1} \cdot q_2^{c_2} \cdot \ldots \cdot q_m^{c_m})} =$$

$$= q_1^{a_1-b_1-c_1} \cdot q_2^{a_2-b_2-c_2} \cdot \ldots \cdot q_m^{a_m-b_m-c_m}$$

Чтобы дополнительно упростить процесс и сократить время вычисления в была так же исследована структура числа сочетаний. В результате анализа разложения биномиальных коэффициентов было получено что: 1) для представления числа сочетаний в канонической форме $C_n^k = q_1^{a_1} \times q_2^{a_2} \times \ldots \times q_j^{a_j} \times \ldots \times q_m^{a_m}$ достаточен набор простых чисел q_j, значения которых не больше n, т.е. п $q_j \le n$ ри $j = 1,2,\ldots,m$; 2) число сочетаний C_n^k в канонической форме записи содержит весь ряд простых чисел, для которого выполняется условие: $q_j \ge n-k+1, k \le \frac{n}{2}$ и $q_j \ge k+1, k > \frac{n}{2}$ для каждого из которых показатель степени будет равен единице $a_j = 1, j = 1,2,\ldots,m$.

В заключение можно сказать, что предложенный подход к вычислению числа сочетаний на основе канонической формы записи позволяет:

1) существенно уменьшить время вычисления числе сочетаний;

2) сократить объём памяти для промежуточных и конечных значений;

3) позволяет упростить построение специализированных устройств вычисления числа сочетаний и нумерационного кодирования.

УДК 621.391

ПОЛІНОМІАЛЬНІ ДИСКРЕТНІ АЛГОРИТМИ ДЕМОДУЛЯЦІЇ ЦИФРОВИХ СИГНАЛІВ В УМОВАХ ДІЇ НЕГАУСОВИХ ЗАВАД

С. В. Заболотній, к.т.н., доцент,
С. В. Салипа, аспірант; О. В. Жигайло, магістрант
Черкаський державний технологічний університет
zabolotni@ukr.net

Відомо, що процес передачі інформації супроводжується дією на корисні сигнали завад різноманітної природи та походження. При застосуванні сигналів із цифровою модуляцією процедуру їх демодуляції трактують як задачу розпізнавання випадкових процесів.

При адитивній моделі взаємодії сигналу і стаціонарної завади та дискретному способі опрацювання рішення базується на аналізі послідовність із N відліків вхідного сигналу, узятих протягом часу його спостереження $y(n)=u_m(n)+x(n)$, $n=\overline{0,N-1}$. Загальна задача полягає у визначенні того, який із можливих M корисних сигналів $u_m(n)$, $m=\overline{1,M}$ присутній в $y(n)$.

При апріорно відомій щільності розподілу завади $p(x)$ і когерентному прийомі оптимальна процедура прийняття рішення базується на обчисленні M статистик максимальної правдоподібності $f_m^{МП}(\vec{y})=\prod_{n=0}^{N-1} p[y(n)-u_m(n)]$. За максимальним значення відповідної m-ої статистики і визначається тип отриманого сигналу.

При найбільш поширеній гаусовій гіпотезі про розподіл завади процедура максимальної правдоподібності спрощується і базується на визначенні мінімальної із

середньоквадратичних статистик $f_m^{CK}(\vec{y}) = \sum_{n=0}^{N-1}[y(n) - u_m(n)]^2$ або на еквівалентному обчисленні M взаємних кореляції функцій між прийнятим сигналом і очікуваними.

В даній роботі для розпізнавання сигналі пропонується використовувати алгоритми, які базуються на властивості мінімізації поліноміальних степеневих статистики виду $f_m^{ПС}(\vec{y}) = \sum_{n=0}^{N-1}\left[\sum_{i=1}^{S} h_i\left([y(n) - u_m(n)]^i - \mu_i\right)\right]^2$, де коефіцієнти h_i, $i = \overline{1,S}$ є оптимальними в сенсі мінімуму середньоквадратичної похибки розкладу завади в стохастичний степеневий ряд, а μ_i, $i = \overline{1,S}$ - центральні моменти завади. Зазначимо, що класичні статистики $f_m^{CK}(\vec{y})$ є окремим випадком відповідних статистик $f_m^{ПС}(\vec{y})$ при $S = 1$ та умові центрованості завади $\mu_1 = 0$.

Математичним підґрунтям такого підходу до побудови систем розпізнавання є використання властивості стохастичних поліномів зменшувати дисперсію випадкових величин, що була обґрунтована професором Ю.П.Кунченко.

Проведений комплекс досліджень, який включає демодуляцію сигналів з амплітудною ASK і фазовою PSK маніпуляцією показав, що в умовах дії негаусових завад, запропоновані поліноміальні алгоритми по ефективності займають проміжне місце між кореляційними алгоритмами та алгоритмами максимальної правдоподібності. Проте у порівнянні з останніми вони володіють тією перевагою, що при своїй побудові використовують статистичні дані про заваду у вигляді послідовності моментів, що значно спрощує реалізацію адаптивності таких процедур.

УДК 519.92

МЕТОД ПІДВИЩЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ КАНАЛУ ПЕРЕДАЧІ ЗА РАХУНОК ВИКОРИСТАННЯ ПОТЕНЦІАЛЬНИХ КОДІВ

М. М. Биков, к.т.н., професор
Т. В. Грищук, к.т.н., доцент
Н. О. Кучерук , здобувач
Вінницький національний технічний університет
nmbdean@ksu.vstu.vinnica.ua

Існуючі методи кодування інформації застосовуються для розробки кодів, що реалізують розрізнювання даних і підвищують ефективність та завадостійкість передачі інформації в каналах зв'язку (наприклад, коди Ріда-Соломона, рангові коди та інш.). В попередніх роботах авторами було доведено достатність інформації про рангові конфігурації станів системи в параметричному просторі для прийняття рішень з управління нею, а також запропоновано метод представлення інформації про стани систем DRP-кодами (distance rank preserving codes - кодами, що зберігають ранги відстаней). Дані коди були названі потенціальними з огляду на аналогію з потенціалами точок електричного поля. У вказаних роботах на прикладах розв'язання практичних задач (ідентифікація станів систем, розпізнавання образів) було показано, що використання запропонованих кодів дозволяє уніфікувати алгоритми прийняття рішень в системах управління з різними методами опису вхідних даних - детерміністичним, імовірнісним, нечітким, наближеним, можливісним та інш. З іншого боку, вказані коди дозволяють значно підвищити пропускну здатність каналу передачі при такому поданні

інформації, оскільки кодові слова містять інформацію як про самі стани обґєктів, так і про ранги відстаней між ними. Було наведено теоретичні основи даного методу кодування, де показано, що застосування таких кодів для передачі інформації про стани систем по каналах зв'язку має обмеження, пов'язані із різким збільшенням розрядності DRP-кодів за умов збільшення кількості станів систем, та з особливостями застосування операцій кодування і декодування рангових конфігурацій систем.

Для усунення згаданих обмежень і підвищення пропускної здатності каналу передачі в роботі розглядається метод передачі інформації, що використовує додаткові властивості запропонованих кодів. Ці властивості випливають з того факту, що за своєю природою потенціальні коди є перестановочними кодами з постійною вагою. Тому запропонований метод передбачає визначення порядкового номера перестановки, що відповідає заданій конфігурації, кодування цього номеру одним із відомих завадостійких кодів, передачу кодового слова по каналу передачі інформації, генерацію рангової конфігурації за отриманим номером і її декодування за допомогою комбінації логічних операцій "AND" і "XOR" в приймачі інформації. Коефіцієнт підвищення пропускної здатності каналу різко збільшується із збільшенням кількості станів системи, про які передається інформація (це може бути, наприклад, інформація про просторову конфігурацію цілей противника, про розміщення мобільних абонентів в бездротовій мережі, про стан нейронної мережі та багато інш.). Наприклад, для системи з 4 станами пропускна здатність каналу підвищується порівняно з відомими методами передачі в 10 раз, для системи з 10 станами – в 55 раз.

УДК 004.7

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ ВИДЕО ДЛЯ ПЕРЕДАЧИ В ПАКЕТНЫХ СЕТЯХ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Д. В. Чепелев, старший преподаватель
Одесский национальный политехнический университет, chepelev@ukr.net

Активное внедрение цифровых систем передачи видео для решения задач дистанционного наблюдения, управления и обучения, делает важным передачу видео в режиме реального времени в пакетных сетях.

На данный момент в качестве основного канала передачи данных используется сеть Интернет, а подключение конечных клиентов все чаще осуществляется посредством радиосетей мобильной связи. Использование этих технологий ведет к следующим проблемам: запаздывание пакетов данных достигает величин 0.6 секунды, порядок их получения отличается от порядка их отправления, значительная часть пакетов может быть потеряна при передаче.

Использование сетевых протоколов с повтором передачи поврежденных пакетов (TCP/IP) позволяет решить проблемы потерянных и неупорядоченных пакетов за счет еще большего, и зачастую непрогнозируемого, ухудшения времени запаздывания данных, что абсолютно неприемлемо для передачи видео в режиме реального времени.

Использование помехоустойчивого кодирования видео позволяет сделать запаздывание прогнозируемой и управляемой величиной. В худшем случае время запаздывания будет составлять время получения всего

набора сетевых пакетов, образующий кодовое слово (будем считать что время декодирования данных мало по сравнению с временем доставки данных). В связи с тем, что потеря одного сетевого пакета ведет к искажению значительного участка кодового слова, целесообразно производить перемешивание битов кодового слова таким образом, чтобы восстанавливающей способности алгоритма было достаточно для восстановления данных. Из-за такого перемешивания битов значительно удлиняется последовательность пакетов содержащая кодовое слово, что ведет к дополнительному запаздыванию видео. Использование алгоритмов с длинным кодовым словом (алг. Рида-Соломона) по сравнению с алгоритмами с коротким кодовым словом (алг. Хэмминга) еще более ухудшает эту ситуацию.

Однако, специфика видеоданных такова, что искажение части этих данных (i-кадры в стандарте mpeg2/4) может всего-лишь незначительно ухудшить их восприятие человеком, либо вообще остаться незамеченным. Что позволяет нам при использовании помехоустойчивого кодирования значительно снизить требования к уровню восстанавливающей способности алгоритмов и использовать алгоритмы с коротким кодовым словом, уменьшая время запаздывания видео. В тоже время, даже незначительное искажение «опорных» кадров (p-кадры в стандарте mpeg2/4) ведет к значительному искажению видео на десятки секунд.

Из приведенного следует, что целесообразно алгоритм помехоустойчивого кодирования видео для передачи в режиме реального времени разрабатывать адаптивным к содержимому потока видео: высокая восстанавливающая способность для малой части важных видеоданных и значительно ниже для прочих данных.

УДК 621.391.25

СИГНАЛЬНО-КОДОВІ КОНСТРУКЦІЇ ДЛЯ СИСТЕМ БЕЗПРОВОДОВОГО ЗВ'ЯЗКУ З ПРОСТОРОВО-ЧАСОВИМ КОДУВАННЯМ

М. О. Іщенко, старший викладач
Одеська національна академія зв'язку ім. О.С. Попова
dima_ischenko@rambler.ru

Сьогодні інтенсивний розвиток систем безпроводового зв'язку, що забезпечують доступ абонентів до ресурсів мереж загального користування (мобільний зв'язок, високошвидкісний Інтернет та ін.) ініціював появу нових методів, що дозволяють забезпечити якісну передачу інформації по каналах безпроводового зв'язку.

До їх числа слід віднести технологію *MIMO*, відповідно до якої передача інформації по каналам радіозв'язку із завмираннями сигналу здійснюється з використанням набору передавальних і приймальних антен. Методи просторово-часового кодування забезпечують кращий обмін між частотною й енергетичною ефективністю та прийняті до уваги при формуванні стандартів третього покоління (стандарти IEEE:802.11, IEEE:802.16) систем мобільного радіозв'язку (*CDMA*-2000, *W-CDMA*) та інших систем безпроводового доступу (*Wi-Fi*, *WiMAX, HSDPA*), що використовують *MIMO*-технології.

Перший зразок такої технології у формі методу «просторово-часового кодування» (ПЧК) був запропонований колективом авторів A. F. Naguib, V. Tarokh, N. Seshadri на чолі з A.R. Calderbank.

Аналіз показав, що іменовані в літературі "просторово-часові коди" є не що інше як сигнально-кодові

конструкції (СКК), в яких сигнали-переносники вибираються з міркувань забезпечення високої швидкості передачі інформації по каналу, а кодування, що сумісне з рознесенням, призначено для підвищення завадостійкості системи зв'язку.

Незважаючи на широке вивчення методів ПЧК для систем безпроводового доступу на основі блокових кодів, у літературі відсутні відомості про параметри і характеристики решітчастих сигнально-кодових конструкцій (РСКК) для систем з ПЧК (відомості про оптимальні сигнали та коди, складових СКК у форматі ПЧК, а також про методи узгодження в єдиній СКК). Тому на основі проведеної оцінки завадостійкості РСКК в каналі із завмираннями. Обґрунтовано доцільність використання критерію максимуму вільної віддалі для находження оптимальних РСКК. На основі даного критерію був розроблений новий метод переборного пошуку оптимальних РСКК. В основі методу лежить знаходження вільної віддалі. Метод базується на моделюванні емулятора кодера-модулятора, що відповідає структурі РСКК. В результаті пошуку отримані характеристики нових РСКК які забезпечують кращі показники ефективності в порівнянні з відомими ПЧК.

Оцінку ефективності системи зв'язку з використанням нових кодів РСКК для систем з ПЧК проведено у відповідності до показників частотної та енергетичної ефективності.

Частотна ефективність системи з ПЧК оцінювалась питомою швидкістю РСКК (сигналами модуляції і швидкістю завадостійкого коду). Енергетична ефективність визначалась на основі експериментального дослідження завадостійкості системи зв'язку.

УДК 681.32

АЛГОРИТМИ КОДУВАННЯ ТА ДЕКОДУВАННЯ НА ОСНОВІ ГАНКЕЛЕВИХ ТА ТОЕПЛІЦЕВИХ МАТРИЦЬ ПРИ ЗАВАДОЗАХИЩЕНОМУ ІНФООБМІНІ

Н. В. Превисокова, асистент
Прикарпатського національного університету імені Василя Стефаника
natvolo@rambler.ru

Одним із шляхів забезпечення достовірності даних в інформаційних системах є використання завадостійкого кодування. У даному напрямі широко застосовуються методи алгебраїчного кодування на основі лінійних блокових кодів. При реалізації процедур кодування в скінченних полях використовуються кодові системи Галуа, які належать до надлишкових завадозахищених кодів. Водночас, використання кодових систем Галуа при виконанні кодування в нескінченних полях потребує розробки відповідних методів та алгоритмів.

Проведені дослідження дозволили встановити ефективність використання повних кодових матриць Галуа, які є ганкелевими або тепліцевими циркулянтами, в якості породжуючих при виконанні операцій кодування $U=QG$ та перевірки повідомлень $UH^T=0$ над полем дійсних чисел. Дані операції реалізуються внаслідок перемноження вектора-повідомлення $Q=(Q_1, Q_2,..., Q_k)$ на циркулянти $G_ц$ та $H_ц$, де $G=[E|G_ц]$, $H=[H_ц|E]$, $GH^T=HG^T=0$, E – одинична діагональна матриця. Використання в якості породжуючої та перевірочної матриць циркулянтів Галуа дозволяє зменшити обчислювальну складність процедур кодування та перевірки повідомлень від n^2 до $n\ log_2 n$ арифметичних

операцій, оскільки для виконання перетворень використовується алгоритм швидкого перетворення Фур'є (ШПФ).

Для перевірки прийнятого повідомлення, виявлення та виправлення помилок використовується синдромний метод декодування.

На основі аналізу структури перевірочної матриці $H_ц$ розроблено алгоритм декодування, на першому етапі якого за допомогою ШПФ обчислюється вектор-синдром S і визначається розміщення помилок. Відповідно до особливостей побудови матриці Галуа $H_ц$ при будь-якій комбінації з допустимої кількості помилок хоча б один елемент вектора-синдрома дорівнює нулю. З метою визначення позицій помилок виконуються такі перетворення: знаходять номери елементів, для яких елементи вектора-синдрома $S_i=0$, та суму рядків у перевірочній матриці H^T з номерами i. В одержаному векторі-сумі номери нульових елементів відповідають позиціям спотворених завадами елементів.

На наступному етапі декодування, коли розміщення помилок відоме, визначаються величини помилок.

Для реалізації запропонованого алгоритму декодування на основі ганкелевих антициклічних або тепліцевих циклічних матриць кодових систем Ґалуа необхідно виконати порядку $n\,log_2 n$ арифметичних операцій для обчислення синдрома у порівнянні із n^2 операцій при використанні перевірочних матриць, які не володіють такою структурою, та порядку n та $n\,log_2 n$ операцій на етапі визначення позицій помилок замість відповідних n^2 та n^3. Таким чином, розроблений алгоритм декодування є простішим, оскільки дозволяє уникнути розв'язування рівняння локаторів та системи нелінійних рівнянь для визначення позицій помилок.

УДК 621.391.019.3

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ОБРАТНОЙ СВЯЗИ НА ДИСТАНЦИОННЫЕ ХАРАКТЕРИСТИКИ НЕСИСТЕМАТИЧЕСКИХ СВЕРТОЧНЫХ КОДОВ

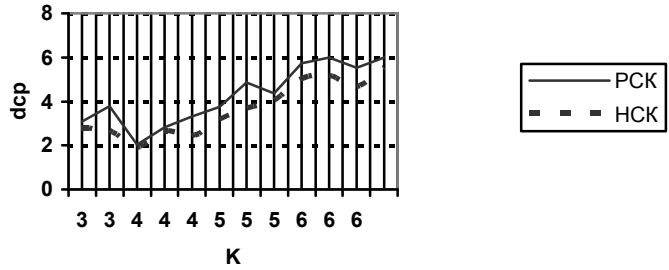
Н. В. Незгазинская, аспирант
Одесская национальная академия связи им.А.С.Попова
natelisk@mail.ru

Сверточные коды (СК) широко применяются в современных цифровых телекоммуникационных системах для повышения помехоустойчивости при действии различных помех. При этом типично использование нерекурсивных сверточных кодов (НСК) (генерируемых кодерами без обратной связи). В последнее время особое внимание обращено на рекурсивные сверточные коды (РСК). Анализ показывает, что переход к рекурсивным кодам позволяет существенно улучшить дистанционные характеристики РСК в сравнении с НСК. Задача доклада – на основе имитационного моделирования дать оценку характеристик РСК. Для исследования использованы программы, разработанные в пакете *HPVEE*. Для исследований были выбраны двоичные СК. Рекурсивный порождающий многочлен РСК может быть выражен через G(D)– исходный нерекурсивный порождающий многочлен и H(D)–многочлен цепи обратной связи следующим образом:

$$G_R(D) = \frac{G(D)}{1 - H(D)}.$$

Для экспериментального определения дистанционных свойств НСК и РСК разработан «метод тест-пакета», основанный на моделировании выходных последовательностей кодера при воздействии на его входе специальным образом сформированного «тест-пакета».

Выходные кодовые последовательности подвергаются анализу для определения минимального расстояния. Программа испытаний содержит датчики порождающих многочленов: датчик многочлена прямой связи G(D) и датчик многочлена цепи обратной связи H(D), вид которого задается случайным образом. Такая методика испытаний позволяла перебрать все возможные варианты действия обратной связи и по результатам усреднения судить о влиянии обратной связи на дистанционные свойства сравниваемых кодов в среднем. Результаты исследований представлены на рисунке. В качестве «опорных» выбирались порождающие многочлены НСК G(D) с различными значениями длины кодирующего регистра К, опубликованные в литературе. По вертикали рисунка отложена величина минимального расстояния $d_{ср}$, определенного методом «тест-пакета» с учетом усреднения по всем возможным реализациям многочлена обратной связи H(D).



Вывод. Экспериментально установлено, что введение обратной связи в кодере сверточного кода увеличивает среднее минимальное расстояние кода. Этот факт служит основанием для организации переборного поиска порождающих многочленов оптимальных РСК.

УДК 621.391.266

МОРФОЛОГИЧЕСКИЕ ОПЕРАТОРЫ ПРЕДВАРИТЕЛЬНОЙ ОБРАБОТКИ ИЗОБРАЖЕНИЙ

Л. В. Рябова, аспирант; Я. С. Яровая, ассистент
Национальный авиационный университет, г.Киев
kzzi@nau.edu.ua

В современном процессе развития информационных технологий обработка видеоинформации становится одной из фундаментальных задач, связанных с машинным зрением, особенно в области автоматизированного визуального контроля. Современная теория многомерной обработки видеосигналов традиционно основывалась на классических принципах теории линейных систем и на преобразованиях Фурье или других ему подобных. Хотя во многих приложениях такие классические подходы анализа оказались весьма плодотворными, однако все они при обработке видеоизображений не позволяют строго аналитически описать геометрические структуры изображения в составе сигналов.

Настоящая работа авторов является логическим продолжением работ по распознаванию статических изображений радужной оболочки глаза пользователя автоматических систем управления доступом. В составе разнообразных алгоритмов обработки видеоизображений различной физической природы можно выделить два обязательных этапа: предварительной обработки и препарирования изображений.

Первый этап, с целью выделения информативных признаков, реализует повышение коэффициента шума исходного машинного кадра методами фильтрации.

Наиболее эффективным, по мнению авторов, является применение нелинейных операторов с использованием теоретико-множественных принципов.

Медианные и рангово-порядковые фильтры стали эффективными нелинейными операторами предварительной обработки дискретных сигналов изображений. Медианные фильтры полезны для устранения импульсного (точечного) шума в изображении, поскольку они позволяют выполнять это без размывания контуров – в отличие от методов линейной фильтрации.

Обобщением методов медианной фильтрации является нелинейные дискретные рангово-порядковые фильтры. Путь реализации двоичных рангово– порядковых фильтров состоит в выполнении линейной свертки двоичного входного сигнала с двоичной импульсной характеристикой, с окном занимающим область $[\boldsymbol{W}] = \boldsymbol{n}$, а затем порогового ограничения получаемого результата на уровне соответствующем рангу $\boldsymbol{r}$. Теоретический анализ таких фильтров затруднен из-за их нелинейности и ненулевой памяти.

Однако, используя теоретико-множественные принципы математической морфологии можно облегчить анализ нелинейных фильтров и предложить для них некоторые новые способы реализации. При этом, преобразование многоуровневого сигнала с помощью морфологических операторов эквивалентно его разложению на все пороговые множества и реконструкции выходного сигнала посредством максимально-пороговой суперпозиции. Такие представления операторов существенно упрощают анализ изображений и определяют альтернативные пути реализации, не требующие цифрового сравнения и сортировки, а следовательно являются более эффективными.

УДК 681.32

СПОСОБЫ ГРАФОВОГО ОПИСАНИЯ ЦИКЛИЧЕСКИХ КОДОВ

В. П. Семеренко, к.т.н., доцент
Винницкий национальный технический университет
VPSemerenko@mail.ru

Каждый алгоритм кодирования и декодирования помехоустойчивых кодов основан на соответствующей модели кода и, поэтому, эффективность алгоритма непосредственно зависит от свойств модели. Наиболее известны следующие методы графового описания циклических кодов: кодовое дерево (КД), Tanner-граф, фактор-граф, кодовая решетка (КР), диаграмма переходов (ДП).

КД представляет собой развернутое во времени и в пространстве представление кодовых слов циклических кодов. В отличие от КД в КР пути могут сливаться и расходиться, если соответствующие кодовые слова имеют в одинаковые моменты времени совпадающие участки, следовательно, КР – это свернутое по пространственному признаку КД. В ДП циклического кода перекрываются между собой пути, которые соответствуют различным кодовым словам в различные моменты времени. Таким образом, ДП – это свернутая по временному признаку КР или свернутое по временному и пространственному признакам КД. Фактор-граф также можно рассматривать как компактное представление КД, однако эта модель удобна для использования лишь при отсутствии циклов.

Свертывание графовых представлений приводит к более компактному представлению циклических кодов и к упрощению процедур кодирования и декодирования.

Однако, с увеличением параметров циклических кодов увеличиваются размеры всех моделей, Поэтому необходим поиск новых способов компактного графового представления кодов.

Предлагаются новые модели циклических кодов на основе теории линейной последовательностной машины (ЛПМ). Граф переходов $G_{FA}(V_{FA}, E_{FA})$ ЛПМ можно рассматривать как совокупность нулевых циклов, соединенных единичными дугами или совокупность единичных циклов, соединенных нулевыми дугами. Из этого графа можно перейти к графу "вертикальных" единичных связей $G_{com}^{z,v}(V_{com}^{z,v}, E_{com}^{z,v})$, либо к графу "вертикальных" нулевых связей $G_{com}^{u,v}(V_{com}^{u,v}, E_{com}^{u,v})$, в котором вершины заменяют соответственно нулевые циклы и единичные циклы. На основе графа $G_{com}^{z,v}(V_{com}^{z,v}, E_{com}^{z,v})$ разработаны алгоритмы декодирования независимых ошибок, а на основе графа $G_{com}^{u,v}(V_{com}^{u,v}, E_{com}^{u,v})$ – алгоритмы декодирования пакетов ошибок.

На основе предложенных моделей проведены оценки корректирующие способности циклических кодов и проведено сравнение с границей Хэмминга и границей Варшамова-Гильберта. Показаны зависимости количества обнаруживаемых и исправляемых ошибок от структуры графовой модели кода для различных классов циклических кодов. Показана возможность исправления независимых ошибок за пределами кодового расстояния .

Введена новая характеристика корректирующих свойств циклических кодов – битовый выигрыш по кодированию.

УДК 621.317

СТРУКТУРА ФІЛЬТРА ДЛЯ СКРЕМБЛЮВАННЯ МОВНИХ СИГНАЛІВ

І. Д. Прокопов, к.т.н., доцент
Вінницький національний технічний університет
alexprokopov@mail.ru

Для скремблювання мовних сигналів використовуються цифрові методи перестановки частотних складових по певному закону з виходу передавача і зворотьні перестановки по тому ж закону на вході приймача. Цифрові методи дають можливість збільшити якісні характеристики цього процесу, але для реалізації їх через ПЛІС-технологію потрібно скоротити кількість обчислювальних операцій і реалізувати їх з меншою кількістю логічних елементів. Скоротити кількість обчислювальних операцій можливо за рахунок використання метода половинного ділення частоти, який дає можливість за рахунок децимації (проріджування) і послідовного зсуву спектра по частоті виконувати спектральний аналіз одним фільтром нижніх частот (ФНЧ). Використовуючи цей метод, а також властивості коефіцієнтів фільтра і позицій однакових значень імпульсної характеристики можливо побудувати структури багатоканальних фільтрів з меншою кількістю логічних елементів. Цифровий нерекурсивний фільтр має симетричну імпульсну характеристику, що дає можливість групувати його коефіцієнти і отримати залежність вихідного сигналу *y(n)* від вхідного *x(n)* у вигляді:

$$y(n) = \sum_{k=2l}^{\frac{M}{2}} h_k (x_{n-k} + x_{n-2M+k}) + \ldots + \sum_{k=2l+1}^{\frac{M}{2}} h_k (x_{n-k} + x_{n-2M+k}) + \ldots + h_M x_{n-M} \quad (1)$$

де l=0,1,2,3… .

Вираз зсуву спектра сигналу по методу половинного ділення має вигляд:

$$X_{ЗС}(n)=X(n)(-1)^n, \qquad (2)$$

де $X_{ЗС}(n)$ - дискретний сигнал з зміненим знаком кожного другого відліку.

Враховуючи, що кожний другий відлік є парним відліком, а у виразі (1) згруповані пари значення добутків коефіцієнтів:

$$\sum_{k=2+1}^{\frac{M}{2}} h_k (x_{n-k} + x_{n-2M+k}) + ... + h_M x_{n-M} (\pm 1)^M \ , \qquad (3)$$

то вираз суми $h_M x_{n-M} (\pm 1)^M$ може мати від'ємне (для високочастотних складових і $(-1)^M h^M x_{n-M}$), чи додатне значення (для низькочастотних складових і $(+1)^M h_M x_n$). Реалізація структур згідно виразу (3) дає можливість скоротити кількість логічних елементів фільтра для реалізації його за ПЛІС-технологією.

Після розрахунку коефіцієнтів ФНЧ , отримують коефіцієнти низькочастотного фільтра в смузі[0;π/3].

Запропонована методика дає можливість розробляти структури багатоканальних фільтрів і реалізовувати їх за ПЛІС-технологією для систем скремблювання мовних сигналів .

УДК 681.325

ОДИНИЧНЕ КОДУВАННЯ ДАНИХ ДЛЯ ВИЗНАЧЕННЯ ЕКСТРЕМАЛЬНИХ ЧИСЕЛ

Т. Б. Мартинюк, к.т.н., доцент
В. В. Хом'юк, к.т.н., доцент
Д. А. Вахромов, студент
Зуріта Рон Андреа Соледад, студент
Вінницький національний технічний університет
chhrroomm@mail.ru

При обробленні сигналів і зображень в алгоритмах фільтрації та кореляції виникає необхідність у визначенні екстремальних значень у масиві даних. При цьому масив може мати вигляд вектора або матриці чисел. У більшості випадків, наприклад, при медіальній фільтрації, застосовують сортування масиву чисел. Але час процедури сортування знаходиться у межах від 0 (m^2) до 0 (m), де m – розмірність векторного масиву чисел, тобто не може бути меншим за розмірність масиву даних. В той же час відомо способи визначення екстремальних чисел у межах 0 ($\log_2 m$).

У випадку, якщо масив даних великий, але числа обмежені за значенням і є цілими числами, можна застосувати апаратний спосіб визначення екстремальних чисел, який полягає в тому, що використовується масив m x n вхідних лічильників, в які записується відповідний масив чисел, вихідний лічильник, з якого зчитується результат, та відповідні логічні елементи. При надходженні тактових імпульсів вміст вхідних лічильників зменшується, а вихідного лічильника збільшується одночасно на одиницю. Процес оброблення закінчується, коли всі вхідні лічильники обнуляться. При цьому за допомогою логічних

елементів можна не тільки визначити екстремальні числа, але й зафіксувати їх місцезнаходження, що є важливим для кореляції сигналів і зображень. Час визначення за таким способом не залежить від розмірності m x n масиву чисел, оскільки вони обробляються одночасно, а визначається величиною максимального числа у масиві.

Якщо замінити двійковий код на одиничний код і замість лічильників ввести зсувні регістри або відомі оптоелектронні багатофункціональні модулі, то можна значно прискорити загальний час оброблення через зменшення тривалості такту τ, оскільки замість реверсивної лічби виконується реверсивний зсув одиниці у межах регістра (модуля).

УДК 519.85:658.846

РОЗРОБКА УДОСКОНАЛЕНОГО МЕТОДУ ПОШУКУ ОПТИМАЛЬНОГО ШЛЯХУ МЕРЕЖЕВОЇ ПЕРЕДАЧІ ДАНИХ У ПРОЦЕСІ ПОБУДОВИ ЗАВАДОСТІЙКИХ КОДІВ

В. В. Войтко, к.т.н., доцент; А. В. Денисюк, асистент
О. В. Гавенко, студент
Вінницький національний технічний університет
vojtko@vstu.vinnica.ua

Розробка методів завадостійкого кодування, орієнтованих на підвищення надійності систем передачі даних, передбачає оцінку базових показників надійності з урахуванням характеристик реальної досліджуваної мережі. Тут важливо врахувати коефіцієнт завантаження мережі, оцінити довжину черги пакетів у робочих вузлах та маршрутизаторах з метою визначення оптимальної кількості надлишкових станів у завадостійких кодових комбінаціях.

Таку оптимізаційну задачу можемо звести до подання вхідних даних за допомогою графа та знаходження оптимального рішення за заданим критерієм. Коли модель розв'язку задачі за початковими умовами вимагає обробки та аналізу усіх складових графа у процесі пошуку оптимальних рішень, то розв'язок зводиться до знаходження оптимального шляху комівояжера в неорієнтованому графі. Тому актуально є розробка удосконаленого методу пошуку оптимального шляху комівояжера в неорієнтованому графі з метою забезпечення умов якісної обробки великих масивів даних у процесі пошуку кінцевого рішення.

Метою роботи є покращення якісних характеристик

методу пошуку шляху комівояжера в неорієнтованому графі у процесі вирішення оптимізаційних задач побудови завадостійких кодів.

Під об'єктом дослідження розуміємо оптимізаційні процеси пошуку кінцевого рішення та формалізацію математичної моделі розв'язку засобами теорії графів. Предметом дослідження є методи пошуку оптимального рішення шляхом використання засобів теорії графів.

Основними задачами роботи вбачаємо удосконалення методу пошуку оптимального шляху комівояжера в неорієнтованому графі шляхом впровадження засобів штучного інтелекту та реалізацію методу в автоматизовані системи пошуку оптимальних рішень.

Серед існуючих методів розв'язку такої задачі популярними є пошук шляху комівояжера за допомогою генетичного алгоритму, який дозволяє обробляти графи великих розмірів, проте не гарантує знаходження саме оптимального шляху комівояжера. Також існує метод гілок та границь, який добре працює для графів малих розмірів, проте є неефективним для опрацювання великих масивів інформації.

Розроблений удосконалений метод пошуку оптимального шляху комівояжера базується на використанні принципів штучного інтелекту. Це дозволяє суттєво зменшити кількість розглянутих варіантів розв'язків за рахунок введення імовірнісних характеристик. Використання запропонованого методу дозволяє збільшити розмір вхідних даних, що обумовлює доцільність його програмної реалізації в автоматизовані системі прийняття рішень, призначеній для розв'язання оптимізаційних задач.

УДК 519.873+004.42

РОЗРОБКА ЗАСОБІВ АВТОМАТИЗАЦІЇ ДОСЛІДЖЕННЯ ЗАВАДОСТІЙКОСТІ МЕРЕЖЕВОЇ ПЕРЕДАЧІ ДАНИХ

С. В. Бевз, к.т.н., доцент; В. В. Войтко, к.т.н., доцент
А. М. Шоботенко, студент
Вінницький національний технічний університет
vojtko@vstu.vinnica.ua

Сьогодні в епоху стрімкого розвитку мережевих технологій, ключовою задачею в галузі формування та передачі інформативних потоків постають проблеми розробки та дослідження засобів завадостійкого кодування. Такі задача потребують комплексного підходу, спрямованого на забезпечення надійності передачі даних за умов мінімізації надлишкових кодових комбінацій. Аналіз надійності та ефективності роботи системи завадостійкого кодування і передачі даних слід проводити з урахуванням взаємозв'язків елементів системи.

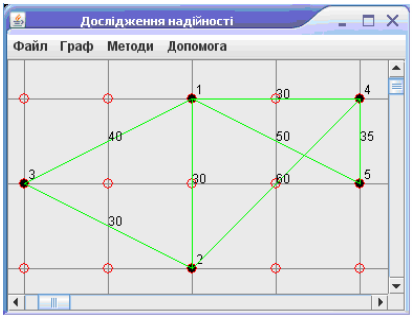
Надійність роботи системи залежить від її структури та складу, способів поєднання елементів системи, їх кількісних характеристик. З огляду на наукове осмислення проблематики надійності складних технічних систем, структурні схеми надійності реальних технічних об'єктів набувають екстенсивного змісту.

Значна частина прикладних задач є ресурсомісткою та вимагає надто складних алгоритмів для обробки об'ємних масивів даних. Частина ж існуючих методів у процесі розв'язку призводить до ускладнення структурних схем опису процесів, що заважає їх алгоритмізації з метою реалізації в автоматизованих комп'ютерних системах. Тому актуальною є розробка методів та алгоритмів

спрощення структурних схем надійності і створення програмного забезпечення для автоматизації процесів розрахунку й оцінювання характеристик надійності.

Метою роботи є автоматизація процесів оцінювання і дослідження надійності складних технічних систем. Об'єктом дослідження є процеси оцінювання надійності технічних систем. Предметом дослідження є методи й алгоритми розрахунку і дослідження надійності технічних систем. Задачею дослідження є розробка моделей та програмного забезпечення автоматизованої системи дослідження надійності складних систем. Методами дослідження є алгоритми розрахунку надійності складних технічних систем, реалізація принципу вкладених матриць у теорії надійності та його дослідження.

Метод вкладених матриць дає змогу отримати матрицю повних взаємозв'язків на основі матриці безпосередніх взаємозв'язків, що формується зі структурної схеми оцінюваної системи. Реалізується



шляхом розбиття матриці на блоки та розгортання симетричної субматриці з поступовим підвищенням порядку за рахунок доповнення елементами вищого рівня. За рахунок таких перетворень отримуємо частину матриці безпосередніх взаємозв'язків. Решта ж елементів знаходиться шляхом заміни базисного вузла та взаємозаміни індексів у вже знайдених формулах ймовірностей.

Програма оперує структурними схемами надійності, здійснює розрахунок узагальнених характеристик надійності та проводить аналіз і моніторинг даних схем.

2. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.432

СИММЕТРИЧНЫЙ БЛОЧНЫЙ RSB-32 КРИПТОГРАФИЧЕСКИЙ АЛГОРИТМ

А. Я. Белецкий, д.т.н., професор
Национальный авиационный университет, Киев
abelnau@ukr.net

Предлагается достаточно гибкий к изменению параметров шифрования (размеров ключей и элементов замены в блоках) симметричный блочный криптографический алгоритм, названный **RSB-32** шифром. Аббревиатура **RSB** происходит от ключевых слов **R**ound, **S**tep, **B**lock подчеркивая тем самым, что основными для криптоалгоритма являются раундовые преобразования (**R**), разбитые на определенное число шагов (**S**), а действие алгоритма осуществляется над блоками (**B**) открытого или закрытого текстов, причем размер базового раундового ключа (как элемента общего ключа или мастер-ключа) составляет 32 бита.

Отличительная особенность **RSB** алгоритма состоит в использовании оригинальных криптографических примитивов, таких как стохастическая круговая прокрутка блоков, лево- и правостороннее «скользящее кодирование» 32-разрядных элементов блоков, нелинейная замена и стохастическая перестановка байтов, которые осуществляются под управлением индивидуальных для каждого шифруемого блока локальных раундовых ключей.

Стохастичность основных операций криптографических преобразований в **RSB** алгоритме обеспечивается не только выбором случайных базовых раундовых ключей, но и домешиванием (в примитиве скользящего кодирования) в локальные раундовые ключи

криптографически преобразуемых (в силу чего приобретающих стохастические свойства) 32–битных элементов шифруемого текста.

Основные параметры **RSB** криптоалгоритма таковы: размер блока шифрования 256 бит; длина раундового ключа 32 бита; длина общего (шагового) ключа $r \cdot 32$, $r = 1, 2, ...$; число шагов шифрования $s = 1, 2, ...$; общее число раундов шифрования $r \cdot s$; размер элементов скользящего кодирования - 32 бита; размер элементов нелинейной замены 8 бит. Длина шифруемого блока легко может быть перестроена до размера $N = 32 \cdot k$, где $k = 2^l$, $l \geq 1$.

Предлагаемый **RSB** алгоритм закладывает реальную основу разработки принципиально новой технологии симметричной блочной криптографической защиты информации в компьютерных сетях. **RSB** криптоалгоритм допускает динамичное управление в широком диапазоне такими параметрами шифрования, как размер блока, длина общего секретного ключа и число шагов (а, следовательно, и раундов) криптографических преобразований. Реализация подобного проекта позволит существенно повысить криптостойкость систем шифрования по сравнению с уже существующими продуктами.

Высокую скорость шифрования в **RSB** технологии можно обеспечить за счет табличных и параллельных способов выполнения основных алгебраических преобразований, а также за счет аппаратной реализации на платформах с 32-х или 64-разрядными шинами.

Эффективность **RSB** алгоритма зашифрования, оцениваемая стандартным пакетом статистической оценки качества шифраторов **NIST STS** (которая приводится в докладе), оказалось на уровне не ниже, а в отдельных случаях превышающем эффективность широко используемых стандартов криптографической защиты, таких как **DES**, **ГОСТ**, **AES** и др.

УДК 004.432

ПОТОЧНЫЙ SPB КРИПТОГРАФИЧЕСКИЙ АЛГОРИТМ ЗАЩИТЫ ЦИФРОВОЙ ИНФОРМАЦИИ

А. Я. Белецкий, д.т.н., професор,
Национальный авиационный университет, Киев
abelnau@ukr.net

Предложен алгоритм синхронного поточного шифрования компьютерных данных, в основу формирования гаммы-функции которого положен принцип стохастического перемешивания элементов 128-битного секретного ключа. Основу алгоритма составляют шенноновские криптопримитивы подстановок и перестановок (**S**ubstitution – **P**ermutation), дополненные операцией стохастического циклического сдвига (Shift) 128-битного блока (**B**lock) шифрующей гаммы. Схема функционирования алгоритма показана на рис. 1.

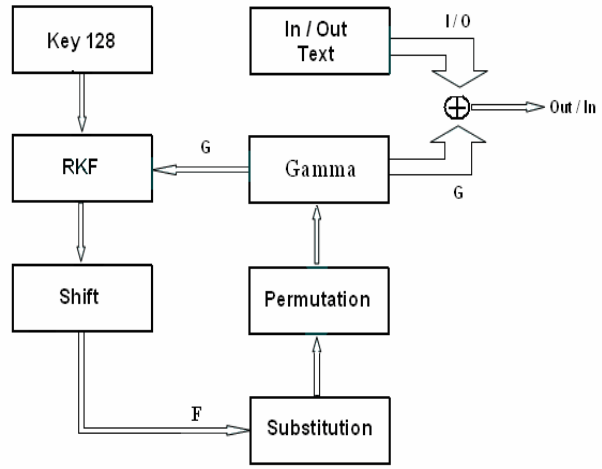


Рис.1. Структурная схема поточного **SPB** криптоалгоритма

На этапе инициализации шифратора секретный 128-битный ключ (**Key** 128) размещается в регистре ключевого поля **RKF**. В блоке **Shift** осуществляется круговой сдвиг содержимого регистра **RKF** на нечетное число $Z \in [1,63]$, которое вычисляется следующим образом. Все 16 байтов регистра **RKF** поразрядно суммируются по mod 2 и в младший разряд результирующего байта $\boldsymbol{B}$ заносится 1 (для обеспечения нечетности). Младшие шесть разрядов байта $\boldsymbol{B}$ и определяют значение параметра прокрутки Z.

Нелинейная подстановка реализуется по классической схеме и отвечает преобразованию байтов $\boldsymbol{x}$ регистра ключевого поля **RKF** соотношением

$$\boldsymbol{y} = (\boldsymbol{x}^{-1} \cdot \boldsymbol{A})_2,$$

где $(a)_2 = a \bmod 2$ – операция приведения результатов матричных вычислений к остатку по $\bmod 2$; $\boldsymbol{x}^{-1}$ – мультипликативное обратное значение байта $\boldsymbol{x}$ над выбранным неприводимым полиномом g; и, наконец, $\boldsymbol{A}$ - невырожденная в кольце вычетов по mod 2 матрица восьмого порядка.

Перестановка байтов выполняется таким образом. Байт, находящийся по адресу $\boldsymbol{X}$ в регистре оператора $\boldsymbol{Sub}$, перемещается в ячейку $\boldsymbol{Y}$ регистра оператора $\boldsymbol{Per}$. Значения $\boldsymbol{Y}$ выбираются из p-й строки таблицы перестановок (размером 16x16), причем номер p определяется содержимым четырех младших разрядов регистра оператора $\boldsymbol{Sub}$. Испытания, проведенные с использование пакета **NIST STS**, подтвердили высокое качество статистических свойств псевдослучайных последовательностей, формируемых предлагаемым поточным шифратором. Алгоритм **SPB** шифрования достаточно простой как в программной, так и аппаратной реализациях, доставляет высокую скорость криптопреобразований и может быть рекомендован для разработки систем поточного шифрования.

УДК 351:65.012.8

МІЖОСОБИСТІСНІ ПСИХОЛОГІЧНІ СТОСУНКИ В АСПЕКТІ ЕФЕКТИВНОСТІ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ

В. А. Янчук[1]
В. М. Журавльов[2], к.т.н., доцент, докторант
[1]Адміністрація Державної прикордонної служби України
[2]НТУУ «КПІ»
[1]YanchukVA@ukr.net, [2]ws_50@mail.zp.ua

Одним із факторів, що впливають на політику безпеки органів державної влади (ОДВ), є характер міжособистісних відносин у середовищі співробітників цих органів, які мають доступ до інформації, що підлягає захисту. Достатньо добре вивчена природа міжособистісних конфліктів, ступінь їх впливу на ефективність роботи персоналу ОДВ. Разом з тим, на думку авторів, завдання ступеня впливу людського фактору у міжособистісних відносинах на забезпечення інформаційної безпеки в ОДВ у періоди кризових явищ у політиці й економіці достатньо актуальна.

Розглядаючи психічні мотиви, можемо виділити три основні типи поведінки особистості (антисоціальна, нарцистична и фанатична поведінка), які є найбільшою загрозою інформаційній безпеці (ІБ) ОДВ. Наявність наступних чотирьох типів поведінки особистості (адитивна, суїцидна, конформіська й аутистична поведінка) у співробітників ОДВ є в тій чи іншій мірі маловірогідною і як наслідок,становить відносну загрозу ІБ ОДВ.

Аналізуючи людський фактор, як один з основних у завдані щодо забезпечення ІБ ОДВ, важливо врахувати можливий прояв своєрідних особистісних якостей окремих співробітників на стан міжособистісних відносин, і, як наслідок, на рівень захищеності інформаційних ресурсів ОДВ. Такі залежності бажано простежувати не тільки для запобігання просоченню інформації з обмеженим доступом, але і для забезпечення її цілісності, доступності, достовірності й спостереженості.

Висновки. Під час аналізу ефективності політики інформаційної безпеки, особливу увагу необхідно звертати на ті психічні особистісні якості співробітників ОДВ, які визначають відношення до: виконання регламентних вимог; виконання вказівок керівництва ОДВ у сфері забезпечення ІБ ОДВ; негативного впливу з боку зовнішнього та внутрішнього середовища функціонування ОДВ; способу оцінки, як своїх дій, так і дій інших співробітників ОДВ; шкідливих звичок; форм і способів відстоювання власної думки; необхідності обліку інтересів інших співробітників ОДВ у процесі ділового та неформального спілкування. Під час проведення заходів, що направлені на розвиток культури державного управління і запобігання, нейтралізацію загроз з боку співробітників ОДВ у сфері ІБ, питанню вивчення психологічних якостей співробітників ОДВ, які мають справу із захищеною інформацією, слід приділяти увагу на усіх етапах кадрової роботи.

УДК 004.056.55, 004.054

СИНТЕЗ СИНДРОМНО ТЕСТИРУЕМЫХ ПОДСТАНОВОЧНЫХ БЛОКОВ ДЛЯ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

Л. В. Дербунович, д.т.н., профессор
Д. Г. Караман[1], аспирант
Д. В. Якубовский[2], аспирант
Национальный технический университет «ХПИ»
[1]karaman.dmitry@gmail.com, [2]bearoff@ukr.net

Современные аппаратные и программные средства систем шифрования обеспечивают защиту больших объемов информации в различных вычислительных и коммуникационных сетях и системах. Однако в последнее время в научно-технических публикациях все чаще поднимается вопрос о надежности реализаций систем шифрования. В частности, особое внимание уделено аппаратным реализациям в виде криптографических модулей и специализированных процессоров. Известно небольшое число работ, связанных с проблемой верификации, тестового и функционального диагностирования таких устройств.

Кроме того, существует еще одна важная причина использования методов технического диагностирования криптографических систем. В последнее время значительно возрос интерес к атакам, направленным на конкретные реализации алгоритмов шифрования. Применение методов тестового и функционального диагностирования позволит своевременно обнаружить факт атаки и предпринять необходимые меры, препятствующие ее проведению.

В докладе предложен метод аппаратной реализации синдромно тестируемых подстановочных блоков S-Box

алгоритма шифрования Rijndael. Определен класс частично однородных схем и достаточные условия их синдромной тестируемости, что позволяет обнаружить кратные неисправности константного типа на входных полюсах логической схемы подстановочного блока и одиночные константные неисправности на всех внутренних его соединениях путем псевдослучайного тестирования и верификации двух спектральных синдромов схемы. Показано, что при синдромной тестируемости ослабляются условия обнаружения ошибок четной кратности по сравнению с методами функционального диагностирования.

Предложен метод логического проектирования многовыходовой схемы подстановочного блока, в которой каждая из восьми функций этого блока реализована частично однородной схемой, процедуры нахождения в этой схеме совместимых выходов, удовлетворяющих условиям синдромной тестируемости и формирование синдромной функции путем суммирования по модулю 2 всех совместимых выходов. В этом случае псевдослучайное тестирование и проверка двух спектральных коэффициентов Уолша синдромной функции позволяет обнаружить 100% одиночных константных неисправностей.

Разработана м о д е л ь синдромно тестируемой реализации подстановочного блока S-Box алгоритма шифрования Rijndael на языке VHDL.

В процессе компьютерного эксперимента моделировались неисправности константного типа в схемной реализации подстановочного блока и эффективность их обнаружения при вычислении синдромов реализуемых функций.

Отмечены достоинства представленного метода аппаратной реализации синдромно тестируемого подстановочного блока и рассмотрены перспективы его использования и развития.

УДК 004.056.5

МОДЕЛІ ТА МЕТОДИ ОПТИМІЗАЦІЇ СИСТЕМ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

А. Д. Кожухівський, д.т.н., професор
А. В. Сагун, к.т.н., доцент
О. А. Кожухівська, аспірант
Черкаський державний технологічний університет
asaha@ukr.net

Постановка задачі. Ефективне функціонування системи інформаційної безпеки (СІБ) підприємства вимагає оснащення комплексом апаратних і програмних засобів захисту (ЗЗ) від різних інформаційних загроз для поліпшення критерію оптимальності створення СІБ.

Виклад основного матеріалу. Припускаємо існування недетермінованої множини інформаційних загрози (ІЗ), що можуть виникнути в автоматизованій інформаційній системі (АІС) підприємства, і недетермінована множина апаратних і програмних засобів захисту. Для кожного поєднання апаратних і програмних засобів захисту (АПЗЗ) визначається $r_1(i, j)$ – ефективність нейтралізації i–м ЗЗ j–ї інформаційної загрози. Для побудови математичної моделі введемо змінну $y(i, j)$ що дорівнює 1, якщо деяка (j–та) ІЗ нейтралізується i–м ЗЗ, в інших випадках є рівною нулю.

Розглядається змістовна та формальна постановка задачі вибору оптимальної СІБ в термінах теорії графів, представлені можливі методи їх розв'язку. Для цього побудований дводолевий граф $G(X,U)$*),* ($X = \cup X_i$, $i = \overline{1,2}$), такий, що вершини множин у X_1 відповідають апаратним і програмним ЗЗ, а вершини множин в X_2 – відповідним ІЗ. Кожний елемент множини X_1

характеризується ціною і ефективністю нейтралізації ІЗ. Тоді завдання вибору оптимальної СІБ полягатиме в максимальній ефективності нейтралізації безлічі інформаційних загроз різними ЗЗ при обмеженнях на обсяги витрат Q виду: $\sum r_2(i) * sign \sum_{i=1}^{n} y(i,y) \le Q$ за умови, що $r_2(i)$ – витрати на придбання i – го ЗЗ.

Постановка задачі з наведеними обмеженнями є лінійною задачею знаходження максимуму цільової функції ефективності нейтралізації ІЗ. Найвищий рівень ефективності СІБ рівний сумі максимальних елементів в кожному стовпці матриці $r_1(i,j)$.

За умови існування стаціонарних розподілів часу між сусідніми змінами параметрів системи захисту і часу отримання несанкціонованого доступу до системи захисту ймовірність подолання перешкоди дорівнює $P_{под} = f\int_0^{\infty}(1-F_{зміни}(t))G_{под}(t)dt$, де $F_{зміни}$ – функція розподілу часу між сусідніми змінами параметрів перешкоди системи захисту; f – величина, обернено пропорційна математичному очікуванню часу між сусідніми змінами параметрів системи захисту; $G_{\text{под.}}$ – функція розподілу часу подолання перешкоди системи захисту. Можливих варіантів для функції розподілу часу між сусідніми змінами параметрів системи захисту перешкоди $F_{\text{зміни}}$ може бути декілька.

Висновки. При створенні найбільш ефективної СІБ для забезпечення протидії НСД в умовах обмежень на ресурси та при визначенні ймовірності спричинення збитків АІС з боку ІЗ може бути використаний наведений вище комплекс оптимізованих математичних моделей.

УДК 621.396.9

СПЕЦИАЛИЗИРОВАННЫЙ «КРИПТОПРОЦЕССОР ОКА»

В. Ю. Ларин[1], к.т.н, доцент; И. А. Павлов[2], студент;
Н. И. Чичикало[2], д.т.н., профессор
[1]Национальный авиационный университет
[2]Донецкий национальный технический университет.
chichikalo@rambler.ru

При совершении несанкционированного доступа к объекту существует глобальная проблема: идентификация и фиксирование момента появления хакера. Многие компании предлагают решения для защиты новое изделие компании Dallas Semiconductor – персональный крипто-процессор DS1957B. Новое устройство – это фактически персональный криптографический компьютер, который обеспечивает управление доступа к Web-страницам, позволяет подписывать документы, шифровать важные файлы, защищать почту Email, и безопасно проводить финансовые транзакции – даже если ваш компьютер, программное обеспечение и линии коммуникаций сомнительны с точки зрения защищенности. Если программное и аппаратное обеспечение подверглись нападению хакера, критическая информация о персональных кодах и шифровальных ключах пользователя останется для него недоступной в физически защищенном чипе iButton. Легко подключив его к порту компьютера, вы можете:

– получить защищенный доступ к конфиден-циальной информации условно-доступных Web-страниц,

– подписывать документы международно-признанными цифровыми сертификатами, так что получатель уверен в подлинности подписи

– шифровать и расшифровать конфиденциальные сообщения для пересылки по Email.

– проводить денежные платежи, выпускать собственные электронные почтовые штампы, печатать и подписывать электронные чеки.

Принцип использования двухфакторной идентификации (иметь что-то + знать что-то) аналогичен тому, что используется в банкоматах. Общая идея заключается в том, что вы носите свой iButton на тщательно охраняемом аксессуаре, и заботитесь о том, чтобы его не потерять.

Предлагаемый способ избавляет от необходимости запоминания секретных паролей, от громоздкой операции ввода ключевых символов, от наличия переносного контактного устройства и наличия с собой компьютера.

Новый «криптопроцессор ОКА» выполнен на жестких параметрических устройствах. Наступайте на него, проходите по нему и т. п. Никаких проблем. Износу не подвержен. Достаточно 100 контактов со считывателем.

Новый «Криптопроцессор ОКА» сохраняет конфиденциальную неклассифицированную информацию. Данный продукт является надежным, физически защищенным модулем для хранения конфиденциальной информации. Позволяет легко обнаружить попытки физического взлома. Память SRAM на монолитном чипе специально сконструирована так, что содержимое уничтожается при попытке вскрытия корпуса.

Доступ к личным ключам в SRAM невозможен, так как взломщик должен преодолеть защитные барьеры других подразделений предприятия и считать содержимое памяти за время, меньшее, чем время, необходимое для стирания содержимого.

УДК 621.391

ОБҐРУНТУВАННЯ ЗАГАЛЬНОГО ПОКАЗНИКА ЕФЕКТИВНОСТІ ОБМІНУ ДАНИМИ В КОМП'ЮТЕРНІЙ МЕРЕЖІ

Д. В. Сумцов[1], к.т.н., доцент
Б. П. Томашевський[2], н.с.
[1]Харківський університет повітряних сил
[2]Львівський інститут СВ
[1]sumtsow@gmail.com

При розгляді функціонування комп'ютерної мережі загальний показник ефективності обміну даними повинен включати показник конфіденційності і приватні показники системи зв'язку – достовірність і оперативність.

Забезпечення конфіденційності (інформаційної скритності) шляхом реалізації механізму захисту інформації може оцінюватися як імовірнісно-часовий показник криптографічної стійкості – безпечний час $T_Б$, що характеризує час безпечної роботи даного криптоалгоритма за умови вживання противником різних методів криптоаналізу. При оцінці критерію достовірності (інформаційній надійності) передачі даних використані кількісні характеристики критерію: вірогідність помилкового прийому одиничного елементу (втратою достовірності), вірогідність помилкового прийому пакету даних, вірогідність правильного прийому одиничного елементу $P_{0\,пр}$ і вірогідність правильного прийому пакету $P_{пр\,n}$. Вірогідність помилкового і правильного прийому одиничного елементу (P_0 и $P_{0\,пр}$) фактично є характеристиками дискретного каналу зв'язку, вірогідність $P_{ош\,n}$ і $P_{пр\,n}$ є характеристиками комп'ютерної мережі в цілому, оскільки вони визначаються не лише характером і

інтенсивністю перешкод в каналі зв'язку, виглядом і швидкістю модуляції, але і способом захисту від помилок в системі.

Для оцінки ефективності функціонування комп'ютерної мережі як показник ефективності введений узагальнений показник функціональної ефективності. Структура побудови показника така, що в ній об'єднано дві основні характеристики системи: необхідна вірогідність досягнення мети з необхідним показником забезпечення конфіденційності (інформаційної скритності) в певних умовах зовнішнього середовища і при певному рівні впливу внутрішніх випадкових чинників, і витрати, які необхідно зробити у вказаних умовах для досягнення мети з необхідною вірогідністю.

Даний показник, включаючи приватні показники достовірності, конфіденційності і часу доставки даних в комп'ютерній мережі, і по суті, відображає швидкість достовірної і конфіденційної передачі даних комп'ютерної мережі, що дозволяє оцінювати ефективність мережі в широкому діапазоні інтенсивностей помилок в каналі передачі даних, при різних швидкостях передачі R.

При цьому окремі показники повинні задовольняти системі обмежень $\{T_{\text{Б}} \geq T_{Д}, P_{ош} \leq P_{Д}, t_{д} \leq t_{Д}\}$, при мінімізації часу доставки кадру інформації.

Вибрані узагальнений показник і критерій ефективності комп'ютерної мережі дозволяють набути чисельних значень, що характеризують швидкість достовірної і конфіденційної передачі даних в комп'ютерній мережі і виробити порівняння існуючих протоколів комп'ютерних мереж по ефективності обміну даними між двома вузлами комп'ютерної мережі.

УДК 004.056:378(147)

ТЕРМІНОЛОГІЯ У ВИЗНАЧЕННІ ПОНЯТЬ СФЕРИ ЗАХИСТУ ІНФОРМАЦІЇ ТА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

М. Г. Коляда[1], к.п.н., доцент;
О. В. Оводенко[2], к.т.н., доцент;
Донецький національний технічний університет
[1]kolyada_mihail@mail.ru, [2]ovodenko@km.ru

Захист інформації являє собою процес чи сукупність методів, засобів і заходів, однак обмежувати спосіб реалізації тільки цим було б невірно. Захист інформації повинен бути системним, а в систему крім методів, засобів і заходів входять і інші компоненти: об'єкти захисту, органи захисту, користувачі інформації. При цьому захист не повинний являти собою щось статичне, а бути безупинним процесом. Але цей процес не здійснюється сам по собі, а відбувається в результаті діяльності людей. Діяльність же містить у собі не тільки процес, але і мету, засоби і результат. Захист інформації не може бути безцільним, безрезультатним і здійснюватися без допомоги визначених засобів. Тому саме діяльність і повинна бути способом реалізації змістовної частини захисту.

Об'єднавши змістовну частину захисту інформації і спосіб реалізації змістовної частини, можна сформулювати наступне визначення: *захист інформації – діяльність по запобіганню втрати і витоку конфіденційної інформації і утрати відкритої інформації, що захищається.*

З поняттям захисту інформації тісно пов'язане поняття безпеки інформації. Термін «*безпека інформації*» (*information security*) має подвійне значення, його можна тлумачити і як безпека самої інформації, і як відсутність

погроз з боку інформації суб'єктам інформаційних відносин. При цьому безпека самої інформації також не вписується в однозначне її розуміння. З одного боку, це може означати безпеку інформації з погляду первісної повноти і надійності інформації, з іншого боку, – захищеність установленого статус-кво інформації.

У словнику «Інформаційна безпека та сучасні мережеві технології» безпека інформації розглядається тільки в розрізі її захищеності, це «стан інформації, в якому забезпечується її невразливість до загроз, що впливають на відповідні характеристики її безпеки». Захищеності від чого? Сюди відносять: від внутрішніх і зовнішніх погроз; від витоку, розкрадання, утрати, несанкціонованого знищення, перекручування, модифікації (підробки), несанкціонованого копіювання, блокування інформації і т.п.; від випадкових чи навмисних несанкціонованих впливів на інформацію чи несанкціонованого її одержання; від випадкового чи навмисного доступу осіб, які не мають права на одержання інформації, її розкриття, модифікацію чи руйнування, та ін.

Інший підхід у визначенні цього поняття можна сформулювати з позиції впливів, що порушують її статус чи від її втрати і витоку. В остаточному підсумку ці підходи виражають одне й те ж саме, тому що запобігання втрати і витоку інформації здійснюється за допомогою запобігання дестабілізуючих впливів на інформацію.

З понять «захист інформації» і «безпека інформації» випливає і співвідношення між ними: *захист інформації спрямований на забезпечення безпеки інформації, з іншого боку, безпека інформації забезпечується за допомогою її захисту*.

УДК 004.056.55

ГЕНЕРАТОР ПСЕВДОВИПАДКОВИХ БІНАРНИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ КЛІТИННИХ АВТОМАТІВ

Л. О. Валь[1], асистент
В. В. Жихаревич[2], старший викладач
С. Е. Остапов[1], д.ф-м.н., професор
[1]Чернівецький національний університет
[2]Чернівецький факультет, Харківського політехнічного інституту
lidval@rambler.ru

Відомо, що криптостійкість потокових шифрів практично повністю визначається якістю генератора ключової послідовності, яка накладається на інформаційний потік, рандомізуючи його. Важливим тут є не тільки можливість відтворення ключової послідовності на приймальній стороні, але й статистичні властивості цієї послідовності, основною з яких є велика подібність послідовності, що генерується, до випадкової. Критерієм такої подібності є, як відомо, неможливість визначення з ймовірністю суттєво більшою, ніж 0.5, яким буде наступний член послідовності, нулем чи одиницею. Не менш важливою вважається відсутність у генерованих послідовностях кореляцій, а також послідовностей з декількох нулів та одиниць, ймовірність появи яких суттєво перевищує 0.5.

В якості генератора псевдовипадкових чисел використовувався одномірний клітинний автомат (КА), який являє собою масив клітин $C_1, C_2, ..., C_n$, стан яких в наступний момент часу визначається за правилом:

$$C_i' = C_{i-1} \oplus (C_i \vee C_{i+1}). \quad (1)$$

Псевдовипадкова послідовність бітів може генеруватися будь-якою з n клітин одномірного масиву.

Для проведення порівняльного аналізу статистичних параметрів генераторів був обраний генератор BBS.

Досліджувався як вплив різних логічних операторів, так і зміна їх порядку слідування в (1). Для кожного випадку виконувався статистичний аналіз, який проводився в два етапи – на першому етапі досліджувалися різні комбінації логічних операторів. Другим етапом досліджень був власне статистичний аналіз відібраних пар операндів та порівняння характеристик псевдовипадкових бінарних послідовностей, які генеруються з допомогою алгоритмів BBS і КА.

Була проаналізована ймовірність генерації двійкових представлень чисел 0, 1, 2, ..., 255. Для обох випадків були згенеровані послідовності з 10.000.000 бітів.

Аналіз періодичних кореляцій, – ймовірність появи «1» на кожному наступному кроці бінарної послідовності (0), через один крок (1), через два кроки (2) і т.д., – показав явну періодичність для ймовірності появи «1» при застосуванні алгоритму BBS.

Базуючись на результатах проведених досліджень можна зробити висновок, що алгоритм КА з комбінацією пар операторів «xor-and» та «xor-or» найкращим чином задовольняє параметрам рівноймовірності появи нуля і одиниці у згенерованій послідовності в порівнянні з BBS. Для підвищення криптографічної стійкості запропоновано спосіб модифікації традиційних КА уведенням псевдовипадкового механізму визначення локалізації взаємодіючих клітин, що разом з високою швидкодією такої схеми, відкриває можливість застосування КА в якості програмних генераторів псевдовипадкових чисел.

УДК 004.056:681.3.06

ПРЕВЕНТИВНИЙ ЗАХИСТ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ МЕТОДАМИ CSS АТАК ТА SQL ІН'ЄКЦІЙ

І. Б. Трегубенко, к.т.н., доцент
Черкаський державний технологічний університет,
irttri@rambler.ru

Атаки які направлені на Web-сервера найчастіше виконуються за технологією CSS атак та SQL ін'єкцій. Принцип дії цих методів заснований на впровадженні зловмисних кодів, мета-символів і SQL команд в URL рядок, що приводить до виконання коду, або у поля введення на Web-сторінках, що змінює виконання кінцевих запитів SQL. Методи превентивного виявлення нападів на базі технологій CSS атак та SQL-ін'єкцій, на відміну від методів запобігання атакам, не напрацьовані.

При організації поліморфного віртуального середовища дослідження безпеки мереж була використана, зокрема, програма IDS Snort і складено регулярні вирази, засновані на правилах для виявлення вказаних видів атак. Задані за умовчанням набір правил Snort містить сигнатури для виявлення сценаріїв CSS атак, але їх можна дуже легко обійти, використовуючи, наприклад, шістнадцяткові значення символів типу %3C%73%63%72%69%70%74%3E замість <script>.

За для виявлення будь-якого варіанту SQL атаки потрібно виключити можливість введення будь-якого з мета-символів SQL типу – одинарної лапки('), крапки з комою (;) або подвійним тире (--). Тотожний метод застосуємо за для виявлення CSS атаки. Він полягає в знаходженні кутових дужок (<>), які вказують на HTML-

тэг. Але за таких умов виникає вірогідність того, що велика кількість правильних виразів, будуть розпізнані як спроби нападів. Необхідно, щоб умови перевірки були більш точними та не призводили до помилкової ідентифікації. Кожна з умов може використовуватися як самостійно, так і з командами Snort сигнатур, використовуючи ключове слово pcre. Ці сигнатури можуть також використовувати з утилітами типу grep для перевірки файлів реєстрації на Web серверах. Але такий мето може використовуватися, тільки якщо додатки використовують GET запити, оскільки дані про POST запитах не зберігаються у файлах реєстрації.

Важливим моментом при виборі регулярного виразу для виявлення SQL ін'єкцій є те, що може ввести зловмисник у полі введення або у полі cookie. Всі данні, яки вводить користувач, необхідно розглядати як підозрілі. Найпростіший регулярний вираз, який використовується для виявлення SQL ін'єкцій, повинен виявляти певні мета-символи SQL типу одинарної лапки або подвійного тире. Для виявлення цих символів і їх шістнадцятиричних еквівалентів може використовуватися наступний вираз: /(%27)|(')|(--)|(%23)|(#)/ix</TD<tr> . В цьому виразі, спершу ми виявляємо шістнадцятиричний еквівалент одинарної лапки або безпосередньо саму лапку, а також присутність подвійного тире. Це символи MS SQL Сервер і Oracle, що позначають початок коментарю. Додатково, у разі використання MYSQL, необхідно перевірити присутність '*' або його шістнадцятиричного еквівалента. Перевіряти шістнадцятиричний еквівалент подвійного тире немає потреби, оскільки він не є мета-символом HTML і не буде закодований браузером. Якщо зловмисник спробує у ручну змінити подвійне тире на його шістнадцятиричний еквівалент (використовуючи проксі типу Achilles), то в атаці за допомогою SQL ін'єкції відбудеться збій.

УДК 004.056.53

ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ АНОМАЛІЙ ТРАФІКУ В ЗАХИЩЕНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

М. М. Гузій, к.т.н., доцент
Національній авіаційний університет, nn05@ukr.net

Проблема виявлення аномалій трафіку комп'ютерної мережі вимагає розробки нових теоретичних підходів, що обумовлене складністю проблеми та її прикладним значенням. Розпізнавання аномалій обчислювальних процесів передбачає вирішення наступних завдань: формування множини еталонів інваріантів нормального розвитку обчислювальних процесів; вибір шкал вимірювання ознак еталонів або інваріантів; обґрунтування достатнього числа інформативних ознак; формування системи правил для розпізнавання аномалій.

У роботах А.Бєляєва, С.Петренко приводиться аналіз принципів, методик і алгоритмів виявлення аномалій, які можуть бути корисні для побудови перспективних систем захисту інформації в комп'ютерних мережах.

Однією з сучасних технологій, від якої чекають певних досягнень є нейромережна технологія. У роботах Ю. Мінаєва показано, що для забезпечення прийнятного рівня ідентифікації атак доцільно використовувати чіткі і нечіткі (fuzzy) нейронні мережі та тензорні моделі трафіка. Виявлення атак на комп'ютерні мережі на підставі аналізу трафіка може бути побудовано шляхом представлення трафіка у вигляді тензора. Тензорне уявлення трафіка дозволяє суттєво підвищити ефективність виявлення його аномалій, зокрема атак.

Результати моделювання показують високу ефективність використання векторних аналогів тензор-трафіка для ідентифікації аномальних станів комп'ютерної мережі. На рис. 1. приведені графічні відображення тензор-трафіка «атака - відсутність атаки» і їх векторні аналоги, побудовані на базі систем ортогональних інваріантів (*sigma*, tau).

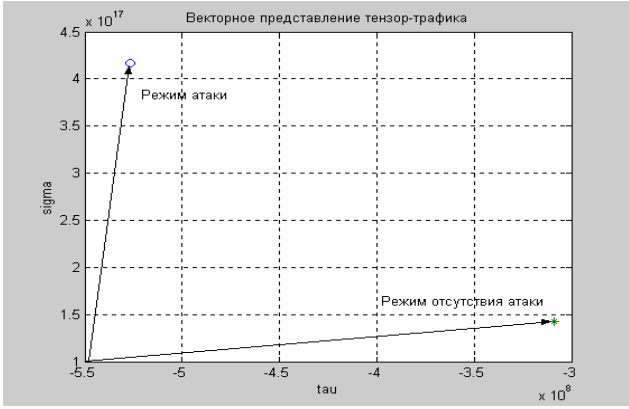


Рис. 1 Відображення тензор-трафіка «атака - відсутність атаки»

Висновки. Трафік комп'ютерної мережі, що представляється у вигляді сукупності параметрів, може бути представлений узагальненим тензор-трафіком, ортогональні інваріанти якого обчислюються на підставі власних значень.

Представлення трафіка комп'ютерної мережі у вигляді тензор-трафіка дозволяє істотно підвищити ефективність ідентифікації аномальних станів комп'ютерної мережі і дозволяє ідентифікувати атаки в умовах невизначеності.

Приведені результати моделювання стану комп'ютерної мережі «атака - відсутність атаки» підтверджують ефективність запропонованої технології.

УДК 621.396.2+519.728

КРИПТОГРАФИЧЕСКАЯ ГИБРИДНАЯ СИСТЕМА DS/FH

В. Я. Чечельницкий, к.т.н., доцент; П. Мурр, аспирант
Одесский национальный политехнический университет
victor@net.opu.ua

В последнее время очень широкое распространение получили беспроводные технологии передачи информации, которые несут с собой гораздо больше угроз безопасности данных, чем проводные системы. Помимо угроз безопасности в радиоканале могут возникать естественные и искусственные ошибки при передаче данных. Поэтому актуальной является разработка помехоустойчивой криптографической беспроводной системы передачи данных.

В беспроводных системах связи широко применяются шумоподобные сигналы, которые обладают высокой помехозащищенностью при действии мощных помех как естественного, так и искусственного характера, позволяют бороться с многолучевым распространением сигналов, обеспечивают лучшее использование спектра частот и электромагнитную совместимость, обладают низкой вероятностью детектирования или же низкой вероятностью перехвата, что обеспечивает скрытность связи.

Гибридная система, которая использует для расширения спектра метод прямой последовательности (Direct Sequence — DS) и метод скачкообразной перестройки частоты (Frequency Hopping — FH) использует преимущества обеих входящих в нее методов расширения спектра.

Метод FH осуществляется традиционным способом, а в качестве расширяющей последовательности для метода DS предлагается использовать сигналы, построенные на базе порождающего класса совершенных двоичных решеток (СДР) порядка $N = 12$. При этом мощность порождающего класса определяется выражением $S(N) = 30\,233\,088$.

Предлагаемый метод криптографической передачи информации состоит из двух основных процедур. Во-первых, информационная модуляция осуществляется путем циклических сдвигов текущей опорной СДР — $H_0(12)$ по строкам и (или) столбцам (эквивалентный класс СДР). Во-вторых, защита информации от несанкционированного доступа обеспечивается тем, что порядок следования опорных СДР $H_0(12)$ из порождающего класса определяется псевдослучайной кодовой последовательностью — *PS*-кодовым словом большой длины, равной мощности порождающего класса. При этом общее число Z различных между собой *PS*-кодовых слов определяется факториальным соотношением $Z = 30\,233\,088!$

На приемной стороне, для решения задачи различения СДР эквивалентного класса достаточно применить единственный, перестраиваемый под текущую СДР — $H_0(12)$ двумерный согласованный фильтр и схему поиска координат максимального пика периодической взаимокорреляционной функции.

В заключение отметим, что каждая текущая опорная СДР никогда не используется повторно, т.е. все ключи равновероятны, при этом количество используемых ключей в точности равно длине сообщения.

УДК 621.396.9

ЗАЩИТА ПРЕСНЫХ ВОДОЕМОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ВОДНОЙ ГЛАДИ

В. И. Купцов, аспирант; А. А. Хижняк, студент;
Н. И. Чичикало, профессор ДонНТУ
Донецкий национальный технический университет
chichikalo@rambler.ru

Традиционные идентификаторы – штриховой код и магнитная полоска обладают такими недостатками, как незначительная информационную емкость, невозможность оперативного изменения записанных данных, большая зависимость от условий эксплуатации, необходимость использования специальных считывающих устройств. К более совершенным средствам относятся электронные идентификаторы – 5 приборов семейства {DS199X} под названием Touch Memory. В их структуре можно выделить четыре основных блока: постоянное запоминающее устройство, блокнотную память, оперативное запоминающее устройство, часы реального времени, а также элемент питания - встроенную литиевую батарейку (сроком службы 10 лет). Стальной корпус используется для осуществления электрических контактов. Он состоит из ободка с донышком (земляной контакт) и электрически изолированной крышки (сигнальный контакт). Для считывания данных из приборов используется контактирующее устройство (зонд), состоящее из двух штампованных металлических деталей, разделенных диэлектриком. Число циклов записи-чтения в статическую оперативную память не ограничено. Так как данные записываются в память в момент касания считывающего

устройства и корпуса прибора, то нарушение электрического контакта в этот момент может привести к разрушению информации в памяти.

Отличительной особенностью предложенного устройства является разработанный способ обмена со считывающим устройством. Для приема-передачи информации используется одна двунаправленная сигнальная линия, состоящая из приводного элемента и звукоснимателя. Протокол обмена данными состоит из трех основных циклов: инициализации, записи и чтения.

Данные передаются по беспроводной линии связи. При передаче данных используется широтноимпульсный метод кодирования, напоминающий азбуку Морзе: в течение одного временного сегмента длинные или короткие состояния логического нуля на линии определяют значение передаваемого разряда со скоростью передачи данных до 16,6 кбит/сек. Достоинством является то, что напряжение питания подается по сигнальной линии данных, что позволяет, сэкономить энергию встроенной литиевой батарейки, считывать память независимо от энергии батарейки.

Простая конструкция приводного элемента и электрического интерфейса позволяют значительно расширить область применения электронного идентификатора по сравнению с традиционными средствами, а в некоторых системах сделать их незаменимыми.

Наиболее широкое применение предложенные устройства находят в системах несанкционированного физического доступа к водной глади пресных водоемов, предназначенных для выращивания товарной рыбы. Ими можно обеспечить защиту доступа в помещения важных объектов, в кабину пилота в самолетах и т.п. Внедрение предложенной разработки существенно отличается от известных и является экономически выгодным.

УДК 621.3

ЩОДО КЕРУВАННЯ КОМПЛЕКСНОЮ СИСТЕМОЮ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ

В. В. Гніліцький[1], к.т.н., доцент;
О. В. Морозов[2], аспірант,
Житомирський державний технологічний університет,
[1]gnil@ztu.edu.ua, [2]zt_oleg_2008@mail.ru

Сучасні інформаційно-телекомунікаційні системи (ІТС), як правило, є територіально розгалуженими системами, які можуть нараховувати велику кількість засобів обчислювальної техніки та різноманітного програмного забезпечення, що в них використовується. Крім того, сучасні вимоги до надійності та безпеки інформації, яка обробляється та зберігається в ІТС, а також інтенсивний ріст інформаційних технологій, призводять до зростання ступені інтеграції різноманітних підсистем, що входять до складу ІТС, ускладнення конфігурацій окремих підсистем та внесення змін в існуючу конфігурацію ІТС.

Надійність роботи ІТС безпосередньо залежить від можливості оперативного керування комплексною системою захисту інформацією в ІТС, що покладається на адміністратора системи. Для ефективного управління ІТС адміністратор повинен здійснювати:

- централізоване управління всіма програмними та технічними засобами (серверами, робочими станціями, активним мережевим обладнанням) ІТС;
- створювати типові конфігурації програмного забезпечення для оперативного налаштування нових технічних засобів;

- здійснювати постійне оновлення програмного забезпечення.

Таким чином існує тісна залежність в роботі ІТС від людини-адміністратора, і те що вона повинна робити постійно.

Для контролю стану комплексної системи захисту інформації в ІТС та можливості допомоги адміністратору у виконанні своїх обов'язків необхідно передбачити здійснення оцінки стану захищеності інформації в ІТС, що передбачає здійснення заходів, спрямованих на виявлення загроз інформації від здійснення несанкціонованих дій в ІТС. Вказане дозволить визначити необхідні заходи щодо керування комплексною системою захисту інформації в ІТС для дотримання визначеної політики безпеки інформації.

Авторами запропоновано порядок проведення оцінки стану захищеності інформації в ІТС та необхідні для цього програмні засоби.

УДК 681.3.06

АВТОМАТИЗАЦИЯ ПРОЦЕССА УПРАВЛЕНИЯ САНКЦИОНИРОВАННЫМ ДОСТУПОМ В ГЕТЕРОГЕННЫХ РАСПРЕДЕЛЕННЫХ БАЗАХ ДАННЫХ

А. А. Блажко, к.т.н., доцент; Сауд Ибаа, аспирант;
Джайяб Т. Д. Альсаффади, аспирант,
Одесский национальный политехнический университет
bblack@inbox.ru

При сопровождении информационных систем (ИС), данные которых расположены на множестве автономных БД, управляемых СУБД от разных производителей (гетерогенные распределенные БД или ГРБД), администраторам приходиться решать трудоемкие задачи: “прозрачно” для пользователей согласовывать содержимое БД и управлять доступом пользователей/ процессов к БД с учетом выбранной политики безопасности. Существует множество решений по согласованию ГРБД с использованием протоколов тиражирования на основе middleware-программных шлюзов или механизмов триггеров СУБД, а также систем управления доступом к данным на основе избирательной или полномочной политик безопасности. В тоже время остается актуальным решать эти задачи в комплексе.

Целью данной работы является автоматизация процесса управления санкционированным доступом к данным со стороны пользователей и процессов согласования ГРБД, позволяющая сократить его трудоемкость администрирования при увеличении размерности БД и количества пользователей.

Унификацию процесса управления предложено проводить на основе модели процесса гетерогенного тиражирования операций согласования ГРБД в виде четверки < *DS, RS, TT, AL* >, где *DS* – граф описания структур распределенных БД; *RS* – множество элементов-описаний схемы тиражирования операций согласования; *TT* – множество элементов-описаний шаблонов программного кода триггеров СУБД по согласованию ГРБД; *AL* – множество элементов-описаний шаблона политики безопасности.

Элемент *AL*-множества представим в виде тройки <*ds, pl, tpl*>, где *ds*∈{*Oracle,DB2,…*} – тип СУБД; pl∈{*DAC,MAC*} – избирательная (*Discretionary Access Control*) или полномочная (*Mandatory Access Control*) политика управления доступом; *tpl* – шаблон команд по управлению доступом, включающий лексемы-константы, предлагаемые конкретными СУБД, и лексемы-переменные вида *user_name, table_name, column_name*.

Элемент *RS*-множества представлен четверкой <*pubdb*, *subdb, ra, trtype* >, где *pubdb, subdb* – БД-издатель, БД-подписчик, соответственно; *ra* – область тиражирования таблиц БД; *trtype* – способ передачи операций согласования (синхронный, асинхронный-*pull*, асинхронный-*push*). В асинхронном-*pull* способе инициатором процесса согласования является БД-подписчик, а при асинхронном-*push* – БД-издатель.

Предложено автоматизировать процессы управления на основе следующих алгоритмов: алгоритм формирования множества *RS,* учитывающий множество *DS* и удовлетворяющий применяемой в организации политике безопасности исходя из *AL*; алгоритм генерации кода процедур согласования ГРБД на основе множества *TT*; алгоритм генерации команд управления доступом на основании множества *AL*.

УДК 004.056.55

ПРИМЕНЕНИЕ СЕТЕЙ КЛЕТОЧНЫХ АВТОМАТОВ В КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ

М. А. Бережная[1], к.т.н., доцент;
Я. Ю. Королева[1], ассистент; И. В. Гормакова[2], аспирант
[1]Харьковский национальный университет радиоэлектроники
[2]Национальный технический университет «ХПИ»
ira.gormakova@mail.ru

Известен ряд работ, посвященных использованию сетей клеточных атоматов (СКА) для реализации блочного и поточного шифрования как в симметричных, так и в ассиметричных криптосистемах.

Такой интерес к СКА обусловлен несколькими причинами. Во-первых, СКА представляют собой однородную структуру, в которой каждая ячейка или клетка взаимодействует только с ближайшими соседями. Отсутствие глобальных обратных связей значительно повышает быстродействие такой сети. Во-вторых, структура клеточного автомата (КА) идентична структуре конфигурируемых логических блоков ПЛИС типа FPGA и поэтому любая СКА может быть легко сконфигурирована в структуре ПЛИС. В-третьих, на основе одномерных СКА легко синтезируются генераторы псевдослучайных последовательностей.

В докладе представлены структуры одно- и двумерных СКА, определены основные свойства СКА, главным из которых является правило настройки или правило эволюции ячеек СКА.

Представлены основные методы построения криптосистем для блочного и поточного шифрования. Показано, что в таких криптосистемах применяются

одномерные СКА, причем для построения блоков шифрования используются две структуры СКА: СКА 1 и СКА 2. Обосновано и доказано, что граф переходов гибридной СКА длиной n с правилами настройки 90, 150 содержит 2^n-1 вершин, т.е такая СКА является генератором всех возможных последовательностей длиной n. Это свойство СКА используется при построении СКА 1.

Обосновано и доказано утверждение, которое определяет групповые свойства гибридной СКА с правилами настройки 51, 153, 195 или с инверсными правилами 204, 102, 60. Показано, что граф переходов состояний для такой СКА имеет циклы равной длины и четной кратности. Групповые свойства СКА используются при построении СКА 2.

Сформулированы требования к тестопригодности СКА. С целью упрощения процедур синтеза проверяющих тестов и диагностирования СКА предложена модифицированная структура сети, в которой для каждой ячейки сети введены дополнительные верхние входы. Определен класс легко тестируемых СКА, для которых предложен метод построения диагностического эксперимента, основанных на концепциях управляемости и наблюдаемости. В диагностическом эксперименте используются две фазы: 1) нахождение и идентификация множества циклических отличительных последовательностей (ЦОП) в СКА; 2) проверка правильности переходов состояний в каждой ячейки сети путем использования ЦОП.

Разработан алгоритм синтеза проверяющих тестов для СКА. Определена верхняя граница длины полного проверяющего эксперимента. Показано, что трудоемкость синтеза проверяющих тестов по предложенному алгоритму в n^2 раз меньше трудоемкости синтеза тестов по тестовому графу ячейки сети, где n – число состояний ячейки сети.

УДК 621.391

МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ АУТЕНТИЧНОСТИ В БАНКОВСКИХ СИСТЕМАХ

С. П. Евсеев[1], к.т.н., доцент; О. Г. Король[2]
Харьковский национальный экономический университет, [1]evseev_serg@inbox.ru, [2]korol_o@mail.ru

Внутриплатежная система (ВПС) банков относится к сложным многоуровневым системам управления критического применения, в которых передача информации требует контроля безопасности на каждом уровне. Важной составной частью ПС предназначенной для обеспечения услуг безопасности, является подсистема криптографической безопасности информации, которая реализуется соответствующими протоколами и механизмами безопасности.

Основные механизмы обеспечения целостности и аутентичности информации в ВПС на различных уровнях (между филиалами, отделениями, центрами и терминалами) и информации, циркулирующей в банковской системе, основаны на использовании стандартов блочно-симметричных шифров (DES, ГОСТ 28147-89).

Особое место среди механизмов защиты занимает цифровая подпись (ЦП), позволяющая реализовать большинство современных схем аутентификации.

Альтернативным вариантом обеспечения целостности и аутентичности являются функции хеширования бесключевые и ключевые, позволяющие обеспечить широкий спектр услуг безопасности информации согласно ISO 7498.

К безключевым хеш-функциям относятся коды выявления изменений сообщения (MDC-Код),

предназначенные для формирования краткого образа или хеш-кода сообщения, который удовлетворяет специальным свойствам и обеспечивает, совместно с другими механизмами, целостность данных. Они делятся на функции, использующие блочные шифры и модульную арифметику.К ключевым хеш-функциям относятся MAC-коды, предназначенные для обеспечения целостности и аутентификации сообщений без использования каких-либо дополнительных механизмов.

Примером являются хеш-функции на базе блочно-симметричных шифров DES, ГОСТ 28147-89, AES. Как известно, стойкие блочные шифры позволяют обеспечить вычислительно стойкие, но не доказуемо стойкие схемы аутентификации.

Другим вариантом обеспечения целостности и аутентичности являются универсальные хеш-функции, победившие на европейском конкурсе криптоалгоритмов НЕССИ 2004 году. Широкую популярность получили схемы ключевого хеширования UMAC на основе полиномиальных функций, которые позволяют получить высокую скорость хеширования. Они основаны на трехуровневых схемах хеша UHASH использующий БСШ AES для кодирования остатка.

Основными достоинствами универсальных хеш-функций являются высокие показатели скорости хеширования (10^9 бит/с). Однако применяемые методы универсального хеширования не позволяют обеспечить криптографическую стойкость к атакам злоумышленника. Практически все функции универсального хеширования применяются в композиции с алгоритмами шифрования, в результате чего обеспечивается стойкость, но теряется свойство универсальности. Таким образом, перспективным направлением дальнейших исследований является разработка новых подходов к разработке стойких универсальных схем хеширования.

УДК 519.725.4+004.932.2

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ВОДЯННЫХ ЗНАКОВ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ МЕДИЦИНСКИХ ИЗОБРАЖЕНИЙ

Л. А. Кузнецова, ст. преподаватель
Одесский национальный политехнический университет
kuzludan@ukr.net

Актуальность информационной безопасности в медицинской информационной системе основывается на средствах обеспечения целостности, подлинности, доступности и конфиденциальности данных. Безопасность медицинских изображений, может быть обеспечена путем использования водяных знаков.

В данной работе предложен алгоритм построения обратимого цифрового водяного знака построенного с использованием кодов, исправляющих ошибки, основанный на модульном сложении с изображением носителя.

Водяной знак, который будет внедряться в изображение, является секретным ключом системы. Использование модульных операций для внедрения водяного знака, позволяет восстановить точное изображение. Для улучшения качества изображения и эффективного обнаружения водяного знака, в работе предложен алгоритм изменения интенсивности водяного знака в зависимости от освещенности различных участков изображения. Построение водяного знака осуществляется на базе кодов, исправляющих ошибки.

Чтобы выбрать соответствующий детектор из предложенных, нам необходимо проанализировать освещенность изображения.

Перед внедрением водяного знака проводится анализ освещенности разных участков изображения для изменения интенсивности внедряемого водяного знака.

При использовании этого подхода, изображения с водяным знаком не могут использоваться «как есть» для медицинских целей из-за видимых искажений. Единственный путь для получения исходных высококачественных изображений – использовать предложенный протокол для хранения, получения, восстановления изображений с водяным знаком. Во время процедуры внедрения мы можем избрать интенсивность водяного знака и детектора, анализируя гистограмму изображения.

В работе рассмотрены различные детекторы цифрового водяного знака, проанализированы критерии максимального подобия и построен адаптивный алгоритм выбора детектора водяного знака с учетом критерия максимального подобия:

$$\Lambda^{MD} = \sum_{n \le N} (((s(n) - \alpha w(n)) \bmod C_m) - C_0)^2 - \sum_{n \le N} (((s(n) + \alpha w(n)) \bmod C_m) - C_0)^2$$

Также предлагается метод уменьшения вычислительного времени, необходимого для инициализации процедуры верификации путем использования заранее определенных кодовых книг для того, чтобы избежать затрат вычислительного времени на их создание каждый раз перед началом процедуры.

УДК 004.932.2

АДАПТИВНЫЙ АЛГОРИТМ ВНЕДРЕНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В МУЛЬТИМЕДИЙНУЮ ИНФОРМАЦИЮ

О. О. Яковенко, старший преподаватель
Н. И. Кушниренко, студент
Одесский национальный политехнический университет
theradix@mail.ru

Внедрение цифровых водяных знаков в мультимедийную информацию открывает новые перспективы в направлениях защиты авторского права и контроля распространения данных.

Дополнительная информация внедряется в мультимедийный контейнер, частично заменяя его содержимое. Алгоритмы внедрения такой информации обычно специфичны для каждого отдельного контейнера.

В работе рассматривается адаптивный алгоритм внедрения цифровых водяных знаков в мультимедийные контейнеры, сжатие информации в которых базируется на алгоритме jpeg.

С целью увеличения помехоустойчивости и эффективности, для внедрения используется область преобразований – изменению подвергаются коэффициенты матрицы дискретного косинусного преобразования (ДКП); это позволяет внести такие изменения в изображение, которые не будут устранены при его сжатии по алгоритму jpeg с заданным качеством.

Используется избирательное внедрение в коэффициенты ДКП. При игнорировании низкочастотных элементов матрицы ДКП, исключаются заметные искажения в изображении. При игнорировании

высокочастотных элементов, сохраняется свойственный для алгоритма jpeg высокий коэффициент сжатия.

Вводится понятие маски – набора коэффициентов матрицы ДКП, которые могут быть изменены в результате внедрения цифрового водяного знака в изображение.

Так как в большинстве естественных или CGI-изображений разные элементы изображения несут разное количество информации, целесообразно использовать несколько масок для элементов изображения с разным количеством информации.

В работе предлагается механизм классификации элементов изображения по среднему количеству визуальной информации, позволяющий сопоставить каждый элемент изображения с одной маской из заданного набора. Такой алгоритм может быть основан как на полном анализе коэффициентов ДКП, так и на самом алгоритме jpeg.

В случае анализа коэффициентов ДКП, элемент изображения классифицируется по количеству визуальной информации с использованием шаблонов.

Во втором случае алгоритм jpeg применяется ко всем элементам изображения по отдельности. Анализируются результаты сжимаемости элементов, и по результату делается вывод о среднем количестве визуальной информации в элементе изображения. На основе этого можно сформулировать рекомендации относительно маски, которая может быть применена к каждому конкретному элементу изображения.

Также формулируются рекомендации относительно набора масок, достаточного для реализации адаптивного внедрения, а также алгоритма сопоставления количества визуальной информации в элементе изображения с одной из масок.

УДК 681.3.07

ДОСЛІДЖЕННЯ КОМП'ЮТЕРНИХ ІНЦИДЕНТІВ У БАНКАХ

Є. А. Завальнюк, к.т.н.
Управління Національного банку України у Вінницькій області

У доповіді розглянуто одну з актуальних проблем інформаційної безпеки – розслідування комп'ютерних інцидентів офіцером безпеки та визначено методику розслідування і формування необхідного інструментарію для оперативного вирішення інциденту.Суб'єктами зловживань з використанням інформаційних технологій можуть бути як співробітники фінансово-господарських структур, так і сторонні особи, що не працюють у банківських структурах - зловмисники. Як показує статистика, останні у більшості випадків працюють самостійно, за власною ініціативою, але не виключається також їх змова з окремими працівниками кредитно-фінансових установ.

Тому загальноприйнятий термін у банківській системі "офіцер безпеки" набуває іншого сенсу - інформаційного. Тільки тоді, коли за захист кожної корпоративної мережі відповідатиме досвідчений офіцер безпеки, що має в своєму розпорядженні необхідні інструменти захисту, можна буде говорити про адекватні заходи щодо можливих комп'ютерних інцидентів.

При дослідженні часто важливим чинником, що дозволяє зберегти необхідну доказову інформацію, є оперативність. Однак експертиза реального комп`ютерного інциденту вимагає деякого часу не тільки для пошуку відповідних фахівців, але й на її здійснення. Саме тому дослідження комп'ютерних інцидентів доводиться проводити тими силами, які існують на поточний момент. У цьому

випадку дослідник сам не застрахований від помилок: завантаження комп'ютера з системи, яка на ньому була встановлена, протягом дослідження, відсутність перевірки комп'ютера на наявність вірусів і програмних закладок, допуск до комп'ютера користувача цього комп'ютера при дослідженні, не відключення комп'ютера, який піддано атаці, від інформаційної мережі фізично, не прийняття можливих заходів для зняття образу жорсткого диску атакованого комп'ютера, тощо.

Методика розслідування комп'ютерного інциденту складається з 6 етапів: отримання оперативної інформації системи (live response), дублювання даних, аналіз отриманих даних, складання звіту і створення рекомендацій, заходи щодо усунення наслідків даного інциденту, заходи щодо запобігання подібних інцидентів в майбутньому.

Фахівець припускає, що не кожна несанкціонована подія вимагає повного дослідження. Зрозуміло, що кожен інцидент вимагає різної послідовності дій. Існують певні типи інформації, які можуть бути зібрані і швидко проаналізовані для того, щоб визначити, які подальші кроки слід зробити.

Жива відповідь дозволяє зібрати короткочасно існуючі дані, які втрачаються, коли машина-жертва вимикається. Жива відповідь може бути єдиним шансом, якщо незалежні від вас обставини не дозволяють вимкнути машину. Така відповідь може бути критично важливою не тільки для визначення подальших дій дослідника, але і з фінансової точки зору. Вимикання системи може виявитися дуже дорогим, тоді як необхідна для визначення природи інциденту інформація може бути легко зібрана без цього. Тому особа, відповідальна за усунення інциденту повинна добре розуміти, яка інформація може і повинна бути зібрана саме на цьому початковому етапі.

Запропоновано варіант набору інструментальних засобів дослідника для отримання живої відповіді (Toolkit Forensic), а також способи застосування цього варіанту в банківській системі.

УДК 681.3

ЗАЩИТА РЕЧЕВОЙ ИНФОРМАЦИИ НА ОСНОВЕ РАСПРЕДЕЛЕНИЯ ДЖОНСОНА

С. Б. Приходько, к.т.н., доцент
А. В. Пухалевич, магистр
Национальный университет кораблестроения
sbp@ustu.edu.ua

В области защиты речевой информации одной из актуальных является проблема нарушения ее конфиденциальности. В компьютерных системах эта проблема решается путем защиты информации с помощью методов криптографии. Однако сейчас, помимо использования хорошо известных криптографических алгоритмов, наблюдается поиск новых решений.

К сравнительно новым решениям в области криптографии можно отнести применение теории детерминированного хаоса. Однако у динамических хаотических систем имеется ряд отрицательных свойств (например, существование непредсказуемо коротких длин орбит), что в криптографии неприемлемо. Другим менее известным решением для защиты речевой информации является применение стохастических дифференциальных уравнений (СДУ). Для защиты речи на основе СДУ был предложен следующий подход. Речевой сигнал или его часть представляется СДУ, причем для нормализации речевых данных применяется преобразование Джонсона семейства S_U. На следующем этапе в результате решения задачи параметрической идентификации находятся коэффициенты СДУ. При передаче вместо речевой информации передаются значения одной из компонент

СДУ, или значения белого шума, полученных из разностных уравнений численного решения СДУ.

Применение преобразования Джонсона для нормализации речевых данных требует расчета параметров данного преобразования для каждой новой реализации речевого сигнала. Поэтому актуальной является задача получения обобщенной плотности вероятности на основе распределения Джонсона, которая была бы применима для практически всех реализаций. Данная задача может быть решена за счет ввода зависимости параметров распределения от физических характеристик абонентского тракта, например, от качества микрофона.

В настоящее время для аппроксимации одномерной плотности вероятности речевого сигнала используется двустороннее гамма-распределение, имеющее в своем составе параметр, зависящий от качества (главным образом, полосы пропускания) абонентского тракта, в основном от качества микрофона. На основе указанной плотности вероятности была построена обобщенная плотность вероятности речевых данных в виде распределения Джонсона из семейства S_U. Это позволило осуществлять нормализацию различных реализаций речевых сигналов и конструирование соответствующих математических моделей речевого сигнала в виде СДУ.

Результаты экспериментальных исследований показали применимость полученной обобщенной функции плотности вероятности для защиты речевой информации.

Качество защиты речевого сигнала подтверждено путем построения сонограмм, которые были получены с помощью программы Cool Edit.

УДК 621.038

ПОСИЛЕННЯ ЗАХИСТУ ФАЙЛІВ ПРИ ЇХ ЗБЕРЕЖЕННІ НА КОМП'ЮТЕРІ

В. Б. Чередниченко, старший викладач Харківського національного університету внутрішніх справ, Сумська філія
vi.chereda@gmail.com

1. Вступ. Ефективна протидія несанкціонованому використанню даних реалізується шляхом застосування багатоступеневого захисту. Одним з бар'єрів доступу до файлу є його криптографічне перетворення та зберігання у зашифрованому вигляді на технічному носії. Метою даної роботи є розгляд методів посилення захищеності файлів шляхом їхнього шифрування користувачем комп'ютера з застосуванням загальновживаних програм Microsoft Office або WinRar та паролів підвищеної довжини.

2. Огляд можливостей захисту даних в ОС Windows. В ОС Windows 2000/XP/2003 (починаючи з версії Professional) для шифрування папок або файлів існує підсистема Encrypting File System (EFS), яка діє у файловій системі NTFS. Для кожного файлу формується унікальний ключ шифрування File Encryption Key (FEK). За допомогою засобу Group Policy підсистему шифрування EFS можна відключати. Програмне оснащення Security Configuration and Analysis ОС Windows конфігуруються тільки з правами доступу Administrator. Користувачі категорії User мають обмежені можливості щодо впливу на конфіденційність власних файлів. В офіційно розповсюджуваних продуктах ОС Windows усіх версій використовується шифрування з 40 або 56 - бітовим ключем. Програмні продукти, які оперують 128 – бітовим паролем,

потрапляють під експортні обмеження, встановлені законодавством США.

3. Шифрування файлів Microsoft Office.

Шифрування перед записом на технічний носій файлів, створених за допомогою програм Microsoft Word, Excel, PowerPoint (версій 2000, XP, 2003), можна здійснювати за наступною процедурою. У відкритому документі треба викликати: меню „Сервис”⇨ „Параметры” ⇨„Безопасность”⇨ „Параметры шифрования для документа». Там до рядка ”пароль для открытия файла” звичайно вводиться кодова послідовність довжиною до 15 символів.

Пропонується для підвищення ступеню захисту збільшити довжину паролю, для чого у закладці „Безопасность” активізувати функцію «Дополнительно». У ній можна вибрати методи шифрування з довжиною паролю 128 символів (алгоритм Microsoft Enhanced Cryptographic Provider та подальші). Пропонується для використання довгої випадкової послідовності створити „ключовий” текстовий файл довжиною 128 випадкових символів та зберегти його на зовнішньому носії. При такому методі довжина паролю більша, ніж у ОС Windows.

4. Шифрування файлів програмою WinRar.

Шифрування графічних та інших типів файлів можна здійснювати програмою WinRar. Шифрування пропонується починати як звичайний стиск, а потім перейти у закладку „Дополнительно” та активізувати „Установить пароль”. Програма WinRar використовує алгоритм AES – 128 та сприймає код відповідної довжини.

Для значного підвищення криптографічної стійкості автором випробувано метод повторного шифрування файлів за допомогою програм Microsoft Office та WinRar. Пропонується „ключові” файли додатково захистити паролем їхнього відкриття довжиною до 15 символів.

УДК 335.01

ОЦІНЮВАННЯ ТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВИНИКНЕННЯ КОНФЛІКТУ

А. В. Дудатьєв, к.т.н., доцент
О. П. Войтович, к.т.н., доцент
Вінницький національний технічний університет
andreysaf60@mail.ru

Створення глобального інформаційного середовища принципово змінило технології використання інформаційних ресурсів та їх взаємозв'язок з різноманітною діяльністю людини. У зв'язку з цим актуальною є задача оцінювання та забезпечення інформаційної безпеки, яка напряму впливає на всі інші види безпеки, зокрема, економічну, техногенну, екологічну тощо. Проблема оцінювання та забезпечення інформаційної безпеки виникає, як наслідок конфлікту, у результаті виконання певних дій з метою несанкціонованого доступу до конфіденційних інформаційних ресурсів. Характерними особливостями таких конфліктів є:

- несанкціонований доступ до інформаційних ресурсів змінює взаємодію між суб'єктом (конкурентом) системи і об'єктом захисту;
- у процесі отримання конфіденційної інформації мета суб'єкта та його спеціальні засоби можуть змінюватись;
- процес отримання конфіденційної інформації, а також ймовірні протидії є у великій мірі невизначеними.

Проблема оцінювання та забезпечення рівня необхідної інформаційної безпеки формулюються, як дві класичні задачі аналізу та синтезу ефективної системи

захисту, які вирішуються як на етапі проектування системи захисту інформації (СЗІ), так і на етапі її експлуатації. Ці задачі пропонується вирішувати комплексно, що формалізується у таких кроках:

- ідентифікація існуючих та ймовірних загроз;
- розробка математичної моделі для оцінювання рівня захищеності об'єкту;
- розробка політики інформаційної безпеки (ПІБ) з урахуванням результатів моделювання;
- синтез оптимальної СЗІ.

Для отримання більш ефективного результату на етапах моделювання, розробки ПІБ і синтезу СЗІ пропонується враховувати, як елемент системи – інформаційно-аналітичну підсистему (ІАП). Результати діяльності ІАП використовуються для підготовки відповідних управлінських рішень які спрямовані на випередження певних дій ймовірних конкурентів та мінімізацію ризиків. Більшість конфліктних ситуацій характеризуються невизначеністю, зокрема, параметричною та процедурною. Це накладає певні особливості щодо використання адекватного математичного апарату для моделювання стану об'єкту захисту на різних етапах його життєдіяльності, та формулює оригінальні задачі, які пов'язані із забезпеченням необхідного рівня безпеки з урахуванням та упередженням дій конкурентів.

У доповіді пропонуються математичні моделі для оцінювання рівня захисту інформаційної безпеки та синтезу СЗІ в умовах конкуренції або конфліктної ситуації. Запропонована математична модель функціонування ІАП за умов виникнення потенційної конфліктної ситуації, дозволяє виконати вибір безконфліктних операцій, зокрема, операцій або дій відносно ресурсів, дозволяє забезпечити стійкість взаємодії об'єкту захисту із оточуючим конкуруючим середовищем.

УДК 681.3.06 : 519.248.681

АНАЛІЗ СТІЙКОСТІ АЛГОРИТМІВ МОНТГОМЕРІ ДО АТАК СПЕЦІАЛЬНОГО ВИДУ

Чайківська Ю.М.[1], асистент; Дубчак Л.О.[2], асистент;
Тимошенко Л.М.[2], к.е.н.
[1]Тернопільський національний педагогічний університет імені Володимира Гнатюка,
[2]Тернопільський національний економічний університет
u_chaika@yahoo.com

Основною операцією в багатьох криптосистемах з відкритим ключем є модулярне множення. Алгоритм Монтгомері дозволяє виконати операцію множення $P = (X \cdot Y\left(2^n\right)^{-1}) \bmod M$. Існують модифікації алгоритму Монтгомері, спрямовані на зменшення часу виконання операцій модулярного множення. Проаналізовано класичний алгоритм Монтгомері (алгоритм 1) та його модифікацію модулярного множення з чергуванням (алгоритм 2).

Для дослідження часової реалізації алгоритмів 1 та 2 необхідно проаналізувати час, затрачений процесором на виконання кожної операції. Нехай t_1 - час, затрачений на виконання простого присвоєння, t_2 - на додавання чи віднімання двох чисел (процесор затрачає на ці дві операції однаковий час), t_3 - час, затрачений на множення чи ділення двох чисел, t_4 — час, затрачений на виконання операції $x \bmod y$, t_5 - на здійснення операції *xor*.

Отже, в загальному випадку час виконання алгоритму1:

$$T1(H(n)) = t_1 + 2nt_2 + H(n)t_3 + \frac{4}{3}nt_2 = t_1 + \frac{10}{3}nt_2 + H(n)t_3\ , \qquad (1)$$

де $H(n)$ — вага Хеммінга (кількість одиниць в бітовому представленні n).

Аналогічно для алгоритму 2 час виконання рівний:

$$\begin{aligned} T_2(H(n)) = 3t_1 + \sum_{i=n-1}^{0}(2(t_1 + (n + H(n))t_4 + (n + H(n))t_4) + 4t_3 + 4t_5 + \\ + 2t_3 + 3t_2 + (n-1)t_3 + t_4) + t_2 + t_4 = 3t_1 + 2nt_1 + 2n(n + \\ + H(n))t_3 + 2n(n + H(n))t_4 + 4nt_3 + 4nt_5 + 2nt_3 + 3nt_3 + \\ + n(n-1)t_3 + nt_4 + t_2 + t_4 = (3 + 2n)t_1 + (3n + 1)t_2 + (6n + \\ + 3n^2 + 2nH(n) - n)t_3 + (2n^2 + 2nH(n) + n + 1)t_4 + 4nt_5 \end{aligned} \qquad (2)$$

На рисунку 1 представлено залежність часу виконання алгоритмів 1, 2 від ваги Хеммінга.

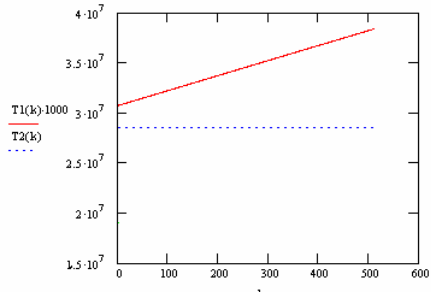


Рисунок 1. Оцінка часових характеристик досліджуваних алгоритмів

З рисунку 1 видно, що алгоритм 2 є стійким до атак спеціального виду, зокрема, часового аналізу та аналізу енергоспоживання. Окрім того, цей алгоритм має прийнятний рівень швидкодії, тому саме його доцільно використовувати на практиці. Для підвищення стійкості можна запропонувати внесення пустих операції в алгоритм, що не вплинуть на результат виконання. Пусті операції дозволяють замінити правильний хід виконання на неправильний.

УДК 62.50

ВИКОРИСТАННЯ ІНТЕРВАЛЬНИХ ФУНКЦІЙ НАЛЕЖНОСТІ ПРИ ОЦІНЮВАННІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

С. М. Куземко, к.т.н., старший викладач
Вінницький національний технічний університет
kuzemko@yandex.ru

Задачу оцінювання ступеня захищеності інформації в сфері інформаційної безпеки можна формалізувати таким чином. Є об'єкт дослідження (наприклад офіс, підприємство, чи інший об'єкт), є певні залежні характеристики. Необхідно визначити кінцеву ступень захищеності об'єкту - число в певному діапазоні, наприклад від нуля до одиниці. Поставлена задача в такому формулюванню є задачею моделювання невідомих залежностей і її можна розв'язувати за допомогою сучасних методів, таких як нейронні мережі та нечіткі логічні системи. Але оскільки предметна галузь може містити велику кількість невизначеностей пов'язаних з відсутністю, або недостатністю верифікованих експериментальних даних, які містять досвід розв'язання поставленої задачі для інших об'єктів, наявністю пропусків як в експериментальних так і вхідних даних, неможливістю отримання точних значень вхідних параметрів, недостатністю вхідної множини параметрів для адекватного відображення об'єкту моделювання, то доцільнішим виглядає використання нечітких логічних моделей на основі інтервальних функцій належності. В цьому випадку в якості вихідної величини моделі буде не точне число, а інтервал значень, за допомогою якого можна адекватно врахувати всі невизначеності, які присутні в предметній галузі.

УДК 681.3:621.394

DDOS-АТАКИ Й МЕТОДИ БОРОТЬБИ З НИМИ

С. М. Цирульник[1], к.т.н., доцент
Д. В. Кисюк[2], асистент
Вінницький національний технічний університет
[1]svom@planeta.vn.ua, [2]kis@vstu.vinnica.ua

Однієї із самих небезпечних погроз є віртуальні DDOS-атаки, непрямі збитки від однієї подібної атаки можуть становити сотні тисяч доларів у день.

DOS-атака і DDOS-атака - це різновиди атак зловмисника на комп'ютерні системи. Їхньою метою є створення таких умов, при яких легітимні (правомірні) користувачі системи не можуть одержати доступ до надаваних системою ресурсам, або цей доступ ускладнений.

Вони особливо небезпечні для компаній, які пов'язані з телеком-ринком, інтернет-магазинів, ресурсів новин і інших компаній, діяльність яких припускає постійний обіг користувачів до ресурсу.

Схематично DDOS-атака виглядає так: на обраний як жертва сервер обрушується величезна кількість помилкових запитів з безлічі комп'ютерів з різних кінців світу. У результаті сервер витрачає всі свої ресурси на обслуговування цих запитів і стає практично недоступним для звичайних користувачів. Цинічність ситуації полягає в тому, що користувачі комп'ютерів, з яких направляються помилкові запити, можуть навіть не підозрювати про те, що їхня машина використовується хакерами. Програми, установлені зловмисниками на цих комп'ютерах, прийнято називати "зомбі". Фахівці з інформаційної безпеки

виділяють наступні види DDOS-атак: UDP flood, TCP flood, TCP SYN flood, Smurf-атака, ICMP flood

Міри протидії DDOS-атакам можна розділити на пасивні й активні, а також на превентивні й реакційні. DDOS-атаку дуже складно виявити й запобігти, оскільки "шкідливі" пакети невідрізняються від "легітимних". Мережні пристрої й традиційні технічні рішення для забезпечення безпеки мережного периметру, такі як міжмережеві екрани й системи виявлення вторгнень (IDS), є важливими компонентами загальної стратегії мережної безпеки, однак одні ці пристрої не забезпечують повного захисту від DDOS-атак. Міжмережеві екрани дозволяють або забороняють проходження мережного трафіку на підставі аналізу різних полів мережних пакетів. Але DDOS-атака може бути успішно реалізована в рамках дозволених міжмережевим екраном потоків трафіка. Тому що трафік DDOS-атаки – це звичайні мережні пакети, кожний з яких окремо собою атаку не представляє, то система IDS не виявить таку атаку. У деяких випадках, при проведенні таких атак використовується підміна IP адрес джерела, через що стає неможливої ідентифікація шкідливого трафіку від конкретного джерела.

Сучасні засоби захисту від DDOS-атак дозволяють із досить високим ступенем ефективності виявити атаку й зменшити або запобігти збитку ресурсам операторів і їхніх клієнтів. Компанія "NVisionGroup" пропонує комплексне рішення для захисту від DDOS-атак на основі технології Cisco Clean Pipes.

Для боротьби з DDOS-атаками необхідно використовувати комбіновані рішення: на рівні сервера, на рівні сервісів сервера, на рівні мережі, на рівні провайдера, на рівні апаратури, на рівні адміністраторів сервера.

УДК 381.3:616-71

ЗАХИСТ ІНФОРМАЦІЇ В INTERNET-СИСТЕМАХ ТЕЛЕМОНІТОРИНГУ СТАНУ ЗДОРОВ'Я ЛЮДИНИ

С. М. Злепко, д.т.н., професор
Н. А. Дудатьєва, аспірант
Вінницький національний технічний університет
andreysaf60@mail.ru

Сучасні інформаційні технології надали можливість реалізувати процес моніторингу стану здоров'я людини, який передбачає постійне дистанційне спостереження, обробку та передачу конфіденційної інформації. Це дозволяє вирішувати проблему своєчасної діагностики без відвідування спеціалізованих медичних закладів, що призводить до значної економії часових та фінансових ресурсів. Проте, поряд з перевагами, які надають засоби мережі Internet для передачі даних моніторингу стану здоров'я людини, постає проблема захисту діагностичної інформації від несанкціонованого доступу та пошкоджень. Адже будь-яке стороннє втручання може значно вплинути на результати обробки діагностичних даних та прийняття рішення щодо стану здоров'я пацієнта.

У докладі запропоновано рішення задачі розробки правил політики інформаційної безпеки в Internet-системах телемоніторингу стану здоров'я людини, а також наведені шляхи їх реалізації, що надасть змогу забезпечити конфіденційність діагностичної інформації. . З цією метою була розроблена математична модель для оцінювання захищеності інформаційних ресурсів та запропонований підхід щодо синтезу оптимальної системи захисту діагностичної інформації.

УДК 681.32

МОДЕЛЮВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

В. П. Семеренко, к.т.н., доцент;
Є. Ю. Панасюк, студент; С. В. Рябокінь, студент
Вінницький національний технічний університет
VPSemerenko@mail.ru

Методи захисту інформації постійно розвиваються, ускладнюються і поступово оформлюються в окрему галузь інформаційних технологій. Математичним апаратом для опису основних законів взаємодії складних систем, за пропозицією видатного кібернетика Дж. фон Неймана, є теорія автоматів. Однак системи захисту інформації характеризуються великим ступенем невизначеності і випадковості, що ускладнює використання точних математичних моделей.

Поява концепції нечітких множин дала можливість її використання в теорії автоматів та теорії алгоритмів.

Під нечітким автоматом Ω будемо розуміти п'ятірку $A = (S, X, Y, \delta, \omega)$, где S, X и Y - непусті кінцеві множини відповідно внутрішніх станів, вхідних сигналів та вихідних сигналів, відображення $\delta : X \to M(S)$ та $\omega : X \to M(Y)$ - нечіткі функції переходів і виходів відповідно. Нечіткий автомат Ω може бути представлений нечіткою програмою, яка виконує нечіткий алгоритм. Під нечітким алгоритмом будемо розуміти упорядковану послідовність нечітких висловлювань, які містять поняття із теорії нечітких множин.

Прикладами апаратної реалізації нечітких автоматів є робототехніка. Вже сьогодні роботи використовуються в

різноманітних сферах, їх широке впровадження в системи захисту інформації, зокрема в засоби біометричного доступу, дозволить підняти ці системи на якісно новий рівень.

Для практичного моделювання нечітких алгоритмів керування та проведення різних експериментів зовсім не обов'язково мати в наявності самі роботи, для цього пропонується скористатись новітніми інформаційними технологіями.

Однією з таких технологій є платформа Microsoft Windows Presentation Foundation (WPF), в якій передбачені нові графічні засоби (включаючи анімацію, тривимірну графіку) і нова мова розмітки XAML. Важливою перевагою WPF є розвинуті можливості багатопотокового програмування для реалізації паралельних алгоритмів.

Для непрофесіоналів в сфері програмування пропонується спеціалізоване середовище розробки Microsoft Robotics Studio. Це середовище є графічною тривимірною моделлю, в якій відображаються дії роботів та об'єктів, що їх оточують. Для представлення алгоритмів поведінки окремих модулів робота використовуються візуальні діаграми на основі мови Visual Programing Language (VPL). Модулями робота можуть бути різноманітні давачі (відстані, дотику, світла та ін.), Web-камери, пристрої GPS-навігації. В контексті робототехніки програма – це сукупність слабкозв'язних компонентів, які паралельно виконуються.

На теперішній час візуальне програмування в Robotics Studio є одним з найкращих інструментів для практичної перевірки реалізації сценаріїв нечітких паралельних алгоритмів керування.

УДК 681.322:621.391

СТЕГАНОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ НА ОСНОВІ ІНТЕГРАЛЬНОГО КРИТЕРІЮ СТІЙКОСТІ ДО АКТИВНИХ JPEG-АТАК

В. В. Лукічов, здобувач
Вінницький національний технічний університет
lukitchov@mail.ru

Коло задач, вирішуваних в межах сучасних комп'ютерних систем (КС), є надзвичайно широким. Однак основне призначення КС полягає у автоматизованому збирані, зберіганні, оброблені та передаванні інформації. Одним з основних аспектів підвищення ефективності КС є забезпечення високого рівня захищеності інформації в її межах. Серед інших напрямків захисту інформації стеганографія має ряд переваг, що обумовлені непомітністю її реалізації.

Стеганографія зображень є галуззю, що дістала стрімкого розвитку протягом останніх десяти років. Її ціль може бути окреслена як таємне та стійке до різноманітних перетворень приховування даних.

Оскільки порушення таємності може призвести до повної втрати повідомлення, то саме зазначена якість задає основні обмеження при проектуванні стегосистеми. Треба відмітити, що відносний характер цього показника обумовлює існування великої кількості критеріїв, ефективність яких неоднакова для різних методів вбудовування. Іншим важливим аспектом є вимога стійкості. Оскільки широко розповсюджені схеми надлишкового кодування з захистом від помилок, то питання робастності може бути вирішено з ефективністю, що визначається достовірністю відновленої інформації.

Таким чином, проектування будь-якої стегосистеми можна розглядати як задачу умовної оптимізації, де цільова функція певним чином пов'язує робастність із ступенем таємності, а обмеження визначають область адекватності критерію. Такий універсальний підхід дозволить забезпечити високу адаптивність до умов безпосереднього функціонування стегосистеми.

У стеганографії зображень особливо розповсюдженою є схема напівсліпого вбудовування де передається лише стегоконтейнер та відомий ключ. Це визначає особливості стегоаналізу, задача якого полягає у бінарній класифікації зображень на основі властивостей, що зазнають найбільших змін при вбудовуванні. Особливо перспективними є критерії на основі методу опорних векторів (МОВ).

Серед методів обробки зображень найбільшою популярністю користуються методи ущільнення. Найбільший коефіцієнт ущільнення здатні забезпечити методи ущільнення з втратами. Стандарт ущільнення JPEG і досі використовується широко, незважаючи на впровадження більш ефективних форматів на основі вейвлет перетворень (наприклад JPEG2000). Така ситуація, вочевидь, обумовлена інертністю концепцій розробки програмного забезпечення у цій сфері, що в свою чергу дозволяє прогнозувати значну тривалість переходу.

Тому як основну активну атаку на стегоконтейнер розглядається ущільнення за JPEG алгоритмом. З іншого боку, стеганографічне використання вейвлет перетворень дає підстави сподіватися на непомітність внесених змін. За допомогою розробленого інтегрального критерію пропонується дослідити комплексний зв'язок між таємністю та робастністю зазначеного використання в області вейвлет перетворень.

УДК 681.3.067

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ АВТОТРАНСПОРТНИХ ЗАСОБІВ

С. М. Цирульник[1], к.т.н., доцент; О. О. Ященко[2], студент;
В. С. Озеранський[3], аспірант
Вінницький національний технічний університет
[1]svom@planeta.vn.ua, [2]oleksiyy@i.ua,
[3]vova@vkkep.vin.ua

На ринку охоронних систем для автотранспорту найбільшою популярністю користуються моделі StarLine 9, ScherKhan 7, Pandora DXL 2500, Tomahawk X5, Stalker MSP-600NB, Kopel KR-800, Sheriff ZX1050.

Більшість існуючих охоронних систем мають наступні функції: увімкнення сигналу тривоги при спрацьовуванні датчиків у режимі охорони; подача сигналів оповіщення про тривогу на брелок зі зворотнім зв'язком; режими імобілізатора та антипограбування, турботаймеру; програмоване двохкрокове вимкнення режиму охорони; програмований персональний код екстреного відключення; блокування двигуна; автоматичний контроль охоронних датчиків з відключенням несправних та сповіщенням про це; індикація причин спрацьовування сигналізації по 9 зонам охорони; індикація несправної зони при ввімкненні режиму охорони; індикація факту спрацьовування сигналізації звуковими сигналами; світлова сигналізація відкритих дверей.

Аналіз технічних даних показує, що в охоронних системах використовую т ь Манчестере та широтно-імпульсне кодування сигналу, що передається, шифрування інформації - оригінальне або Keeloq; довжина передаваємого коду – 40, 56, 64, 96 біт (в залежності від

виробника), довжина зашифрованої частини – 32 біта; робоча частота – 433,92 МГц; тип модуляції – АМ амплітудна, FSK частотна маніпуляція, QFSK фазочастотна маніпуляція; швидкість передачі даних – від 120мс до 2400 мс.

Проаналізувавши роботу сигналізації Star Line 9 можна побачити, що кодова посилка як зі сторони брелка, так і зі сторони базового блоку має довжину 64 інформаційних біти. Вона повторюється по 5 разів в серії, при цьому від брелка до бази іде всього одна серія, а від бази до брелка – три. При передачі команди, брелок видає зашифрований код, який містить інформацію про команду і передбачене базовим блоком під час попереднього сигналу секретне число. Для шифрування використовується однаковий і незмінний для всіх виробів даної моделі ключ. Перед виконанням команди базовий блок звіряє секретне число з тим, що було надіслано брелку і якщо воно не співпадає не виконує команду.

Доступ до системи Star Line 9 можна отримати перехопивши кодову посилку і не пропустивши її до базового блоку. Кодову посилку можна підібрати перебором, тому що базовий блок весь час очікує одне й теж секретне число ,й не змінює його до тих пір, поки не отримує його від брелка. Зчитавши програму мікроконтролера з брелка або базового блоку автосигналізації цієї моделі можна отримати доступ до усіх охоронних систем даної модельної лінійки.

Для підвищення захищеності транспортних засобів доцільно використовувати охоронні системи з діалоговим протокол обміну даними між брелком та базовим блоком, який повинний складатись з статичної та динамічної частини кодової посилки та застосовувати нестандартні підходи до кодування сигналу.

УДК 681.322

СПОСІБ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ З ПІДВИЩЕНИМ КРИПТОГРАФІЧНИМ ЗАХИСТОМ ТА ШВИДКИМ ДЕКОДУВАННЯМ

О. М. Бевз, асистент
Вінницький національний технічний університет,
sederem1b3@km.ru

В усіх сферах життя та праці людини комп'ютерні системи управління знаходять широке використання. Їх основна мета накопичувати, зберігати та передавати різноманітну інформацію. В більшості випадків, а саме при передаванні, інформація повинна бути захищена від несанкціонованого доступу. Вирішенням цієї проблеми займається криптографія. Ця наука на сьогодні представляє дуже широкий вибір різноманітних систем захисту за допомогою шифрування даних та подальшого його дешифрування після передачі.

Для цілі шифрування має сенс використовувати систему шифрування, що створена на архітектурі дворівневої підстановочно-перестановочної мережі з S-боксами на основі високонелінійних бульових функцій та кодами з максимальною відстанню в якості лінійного перетворення. Така система має криптографічну стійкість до лінійного та диференційного криптоаналізу на 60-80% більшу за стійкість стандарту AES, а швидкість шифрування вища на 5 – 44% за швидкості найпоширеніших алгоритмів шифруваня.

Але крім цього при передаванні інформації існують завади і для отримання неспотворених даних необхідно використовувати кодування. Для передавання інформації потрібні коди, які виправляють не менш як дві

помилки. До таких кодів відноситься сімейство кодів Боуза-Чоудхурі-Хоквінгема. Ці коди дозволяють виправляти будь-яку кількість помилок. Цей варіант кодів БЧХ цілком підходить для вирішення поставленої задачі. Декодування кодової послідовності базується на вирішенні системи рівнянь

$$\begin{cases} z_1 = i + j, \\ z_2 = i^3 + j^3; \end{cases}$$

Існуючі методи розв`язку цієї системи потребують використання регістрів зсуву та декількох циклів, що займає досить багато обчислювального часу.

Формування алгоритму для рішення цієї системи рівнянь з часом роботи менше, ніж у відомих алгоритмах і є головною вимогою до поставленого завдання.

Для рішення квадратного рівняння пропонується перебирати значення і з усіх можливих значень поля $GF(2^4)$. Для того щоб корені були розв'язками системи вони повинні задовольняти обидва рівняння цієї системи. Тут виникає проблема - операція піднесення до кубу (в даному полі) є складною операцією. Для усунення цієї проблеми слід застосувати таблицю відповідності вектора поля його кубу.

Отже знайшовши відповідні значення кубів для потенціальних коренів по таблиці і підставити в систему. Такий метод знаходження коренів є швидший на на 20%, оскільки містить у собі тільки операцію додавання. Розроблена система передавання інформації демонструє зниження часу декодування на 20% та підвищення криптографічної стійкості на 60-80%. Але етап декодування має певні недоліки, які полягають у необхідності додаткового об'єму пам'яті (для зберігання таблиць).

УДК 681.32

КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ НА ОСНОВІ АЛГЕБРАЇЧНИХ ПОРІВНЯНЬ

А. В. Лужецький, д.т.н., професор
М. Л. Гаєвський, магістрант
Вінницький національний технічний університет
gaevskyy@ukr.net

Останнім часом багато вчених відходять від стандартних методів побудови блокових шифрів. Основою багатьох таких методів є використання різних теоретико числових перетворень. Основна ідея запропонованого способу шифрування полягає у виконанні обчислень з використанням матриці Уолша:

$$\mathbf{C} = (\mathbf{H} \times \mathbf{M}) \bmod m,$$
$$\mathbf{M} = (\mathbf{H} \times \mathbf{C}) \bmod m,$$

де **H** – матриця Уолша порядку N;

M – вектор відкритого повідомлення;

m – модуль;

C – вектор зашифрованого повідомлення.

Вектор відкритого повідомлення **M** складається з даних розрядністю n:

$$\mathbf{M} = \{m_1, m_2, ..., m_g\},$$

де m_i – дані розрядністю n.

У запропонованому способі існують два змінних параметри перетворення, які залежать від секретного ключа K: N – розмірність перетворень, який визначається функцією f_1(K), і n – розрядність даних, який визначається функцією f_2(K).

$$\mathrm{N} = f_1(\mathrm{K})$$
$$\mathrm{n} = f_2(\mathrm{K})$$

Розрядність блоку L дорівнює добутку розмірності перетворення та розрядності даних.

$$L = N \cdot n$$

Таким чином, розрядність блоку L також змінна величина.

Для забезпечення оптимального рівня крипостійкості та швидкості шифрування даних рекомендується виконувати 12 раундів перетворень. Розшифрування повідомлення виконується в зворотному до зашифрування порядку.

Для визначення змінних параметрів перетворення рекомендується використовувати лінійний регістр зсуву зі зворотнім зв'язком. Початковий стан регістра представляє собою секретний ключ. Оскільки стандартом AES рекомендується використовувати секретний ключ розміром не менше 128 розрядів, пропонується використовувати такий поліном для побудови лінійного регістра зсуву зі зворотнім зв'язком:

$$x^{128} + x^7 + x^2 + x + 1 = 0$$

Такий генератор випадкових чисел буде мати максимальний період:

$$T = 2^{128} - 1$$

Вихідна послідовність псевдовипадкових чисел ділиться на послідовності по 5 біт, 3 з яких визначають розмірність перетворень, а 2 – розрядність даних. Можливі варіанти розмірності перетворень такі:

2, 4, 8, 16, 32, 64, 128, 256.

Можливі варіанти розрядності даних:

8, 16, 32, 64

Перевагою швидкого перетворення Уолша є те, що його реалізація вимагає тільки операцій додавання і віднімання в кількості $N \cdot \log_2 N$, що забезпечує достатньо високу швидкість шифрування інформації.

УДК 681.32

БЛОКОВИЙ ШИФР НА ОСНОВІ НЕДЕРМІНОВАНОГО АЛГОРИТМУ

В. А. Лужецький, д. т. н., професор
А. В. Остапенко, магістрант
Вінницький національний технічний університет
asja87@gmail.com

Постійно зростаючі вимоги до шифрів, врахування ними особливості сучасної елементної бази обумовлює потребу у створенні нових підходів до реалізації блокових шифрів. Пропонується будувати блоковий шифр на основі використання недетермінованих алгоритмів. Ідея цього підходу полягає в тому, що перетворення на кожному із раундів складається з елементарних перетворень набір і послідовність виконання яких визначаються певними ознаками, що формуються з ключової інформації.

З точки зору секретних систем за Шеноном даний блоковий шифр можна представити як комбінацію «взваженої суми» та «добутку», тобто :

$$S=\prod_{i=1}^{n}\ (\sum_{j=1}^{m} p_{ij}\cdot T_{ij}),\ \sum_{j=1}^{m} p_{ij}=1,$$

де T_{ij} – *ij*-а секретна система;

p_{ij} – ймовірність вибору *ij*-ї секретної системи.

Основними аспектами розробки даного підходу є реалізація механізму формування ознак та створення множини базових мікроопераций. Тобто для нього буде введена множина яка буде характеризувати вигляд функції перетворення F на певному етапі алгоритму. Тоді:

$$P_r=F_q\,(C_k,\ K_k),\ P=\{F_1,\ F_{2,\ldots},F_L\},$$

де F_l – множина різних за виглядом функцій перетворення визначених ознакою q, $(i=1\ldots L)$, P_r – раундові перетворення, r – кількість раундів.

В такому випадку залежно від ознаки q на базі використання множини мікрооперацій буде формуватися певний вигляд функції перетворення F та алгоритму шифрування в цілому.

Для побудови недетермінованих алгоритмів пропонується система базових мікрооперацій в якій виділяються два основних вида мікрооперацій:

- одноопераднді (циклічний зсув на k біт (вліво, вправо), інвертування);
- двоопераднді(додавання за модулем 2 та 2^n).

На основі визначених видів базових мікрооперацій можна побудувати базові структури операцій та описати графічно і мнемонічно можливі реалізації різноманітних раундових перетворень, що забезпечить достатню кількість варіантів для оперування у блоковому шифрі.

Множина ознак включає три вида ознак серед яких:

- ознака визначення виду перетворення (256 варіантів);
- ознака визначення кількості оброблюваних підблоків (2,3,4,5);
- ознака визначення розрядності підблоку (8, 16,32, 64 біт).

З використанням вищеописаних ознак може бути побудовано $4 \cdot 4 \cdot 256 = 4096$ різних алгоритмів для одного раунду перетворення.

Запропонований набір базових мікрооперацій та видів ознак дозволяє створювати високошвидкісні блокові шифри з достатньо простою програмною та апаратною реалізацією.

УДК 681.322:621.391

ДЕТЕКТУВАННЯ СТЕГАНОГРАФІЧНОГО ВМІСТУ В УЩІЛЬНЕНИХ З ВТРАТАМИ ДАНИХ

Є. А. Золотавкін, здобувач
Вінницький національний технічний університет
zhzolot@rambler.ru

Захист інформації є галуззю з стрімким розвитком, що обумовлює появу нових напрямків у ній. Стеганографія є відносно новими, однак багатообіцяючими напрямком, тому розробка та вдосконалення стеганографічних систем є особливо актуальною.

Розвиток інформаційних технологій спричиняє зростання частки мультимедійного контенту в загальному інформаційному потоці. Особливість захисту мультимедійних файлів визначається їх значним розміром. Тому розповсюджений підхід захисту інформації – шифрування – вимагатиме надмірних обчислювальних затрат. У випадку порушення умов використання об’єктів, необхідно довести право власності на них, що дозволяє стеганографічний захист, який реалізується шляхом вбудовування цифрових водяних знаків (ЦВЗ).

Також однією з найбільш обґрунтованих областей стеганографічного використання є прихований зв’язок. Використання мультимедійних файлів для приховування даних, що не мають безпосереднього відношення до них, є доцільним, наприклад, для додаткового захисту криптосистем, де зберігання та передавання ключа є одним з критичних аспектів.

Вдосконалення методів стеганографічного захисту як стосовно цифрових прав, так і прихованого зв’язку, відбувається шляхом підвищення стійкості до пасивних та

активних атак, що в свою чергу передбачає покращення якостей робастності та таємності. В більшості випадків підвищення ефективності вбудовування реалізується за рахунок розробки нових робастних схем вбудовування.

З іншого боку розробка методів таємного вбудовування дозволяє забезпечити цілісність вбудованих даних відмінним від робастного підходу шляхом: якщо місцеположення таємних даних в об'єкті невідоме, його руйнування можливе лише за умови значних спотворень.

Задачу розробки системи вбудовування даних, стійкої до пасивних атак, можна сформулювати як оптимізацію пропускної здатності таємного каналу за умови забезпечення таємності. Для цього необхідно попередньо визначити критерій стеганографічної таємності.

Більшість мультимедійних об'єктів зазнають стандартних для свого класу перетворень, що в основному представлені методами стиснення даних з втратами. З одного боку це зменшує ентропію та обмежує можливості вбудовування, з іншого – дозволяє вносити зміни. Словникові методи ущільнення є одними з найбільш розповсюджених. При цьому вибір кодового слова для кодування будь-якої послідовності символів має бути обґрунтованим, що пояснюється можливістю існування кращих альтернатив. Оскільки внаслідок вбудовування даних під час ущільнення змінюється відповідність співставлення послідовностей, запропоновано стеганалітичний критерій, що використовує оцінку відповідності співставлення кожного кодового слова.

Розроблений стеганалітичний критерій можна використовувати для оптимізації пропускної здатності таємного каналу, що дозволить підвищити ефективність стеганографічного захисту.

УДК 681.3

СИСТЕМА ОХОРОНИ ПЕРИМЕТРУ, НА БАЗІ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

О. П. Войтович[1], к.т.н, доцент
В. В. М'яснянкін[2]
[1]Вінницький національний технічний університет
[2]ТОВ «Арісент Україна»
jbumajnikov@ukr.net

Для забезпечення конфіденційності та цілісності інформації, що представлена у вигляді предметів, нанесена на папері або збережена в електронному вигляді і знаходиться на території певного об'єкту застосовують комплексні системи захисту, які включають блоки спостереження, аналізу, прийняття рішень, виконання певних дій, у відповідності до прийнятого рішення.

Зазвичай блок спостереження – це сенсор. Блоки аналізу, прийняття рішень та виконання певних дій найчастіше представлені певною групою осіб або однією особою, тобто надійність такої системи залежить від людського фактору, і є набагато нижчою в порівнянні із такою, в якій усі блоки реалізовані автоматично.

В попередньо описаній системі є ще два ключових недоліки. По-перше, усі сенсори передають отриману інформацію на сервер для обробки за допомогою дротового з'єднання, що звужує спектр можливих місць встановлення даних сенсорів у випадку складності або неможливості прокладання кабелю. По-друге інформація з усіх сенсорів передається лише в один центр аналізу, який може бути представлений одним сервером або кількома, але такий центр є територіально одним цілим незалежно від кількості і виду об'єктів, що його формують, що також зменшую його надійність.

Варіант системи комплексного захисту, що представляється в даній доповіді забезпечує можливість уникнути усіх трьох описаних вище недоліків:

- участь людини в роботі даної системи мінімальна – налаштування та періодичний огляд для підтримання її у відповідному стані;
- блок аналізу розподілений як територіально так і логічно, тобто блок сенсору може одночасно виконувати свої прямі «обов'язки» і, при необхідності – обов'язки аналізатора, системи прийняття рішень;
- зв'язок між сенсорами базується на основі бездротових технологій.

Це досягається за рахунок використання сенсорних мереж, що утворюються за рахунок безконтактних сенсорів.

До позитивних моментів можна віднести можливість самонавчання як усієї системи, так і її окремих логічних частин. Також варто підкреслити можливість внесення в систему нових сенсорів, видалення або заміна існуючих без значної зміни налаштування існуючої системи.

Для реалізації систем аналізу та прийняття рішень, мережа, що утворюється системою сенсорів працює за принципом нейронної мережі. Тобто кожен сенсор системи представлений нейроном віртуальної нейронної мережі, яка і виконує роль аналізатора та системи прийняття рішень.

Взаємодія між елементами такої мережі може здійснюватись за допомогою спеціально розробленого протоколу на базі шумоподібного сигналу. В подальшій роботі планується дослідити можливість вбудовування засобів стиснення та шифрування повідомлень, що передаються в мережі, що дозволить підвищити надійність та швидкодію системи.

УДК 621.391

ФІШИНГ АБО ІНТЕРНЕТ ШАХРАЙСТВО. МЕТОДИ БОРОТЬБИ ЗІ СТОРОНИ КЛІЄНТА ТА СЕРВЕРА

С. В. Князюк, інженер
Вінницький національний технічний університет
univer@svk.org.ua

Найбільш розвинутою формою Інтернет шахрайства, без сумніву, вважається фішинг. Звичайними інструментами фішингу є використання mail (поштові повідомлення, що використовують методи соціальної інженерії), спеціально розроблені web-сайти і засоби зв'язку.

Все більш універсальними стають методи атак шахраїв, підвищується рівень підготовленості атак з метою крадіжки номерів кредитних карт, банківських рахунків та іншої конфіденційної інформації. За даними звіту APWG (Anti-Phishing Work Group) в місяць виявляється 20109 фішингових розсилок, 11976 фішерських веб-ресурсів.

За останні роки використання Інтернету в країнах СНД досягло такого масштабу, що люди починають довіряти і здійснювати фінансові операції через Інтернет. Це і стало причиною активного розвитку фішингу та інших методів Інтернет шахрайства. Якщо вірити прогнозам дослідницьких компаній, то до кінця 2010 року фінансові операції з використанням глобальної мережі в СНД досягнуть європейського і американського рівнів. До такого зростання активно готуються «інтернет-пірати» і, у свою чергу, варто підготуватися як організаторам ресурсів (сервісів), так і їх користувачам.

Максимальна ефективність боротьби з фішингом досягається за участю користувача. Дуже важливим

вважається дотримання всіх правил організаційного захисту інформації при обміні важливими чи цінними даними. Тому варто відзначити, що інформація всіма зусиллями винна бути донесла до користувачів, як в загальній формі, так і індивідуально від кожного ресурсу.

З своєї ж сторони власник, адміністратор сайту, ресурсу, серверу повинен вжити певних заходів захисту, які включають все - починаючи з одноразових паролів і SSl сертифікатів, закінчуючи методами двосторонньої аунтентифікації і клієнтськими програмами.

Розглянемо детальні інструкції для запобігання помилок, як людського фактору, так і програмного забезпечення для організації валютних операцій за допомогою засобів радіозв'язку та Інтернет. Цим же визначимо що найважливіше в захисті від даного типу Інтернет шахрайства, як Інтернет Фішинг і його різновиди (фармінг, вішинг і т.п.)

УДК 681.327

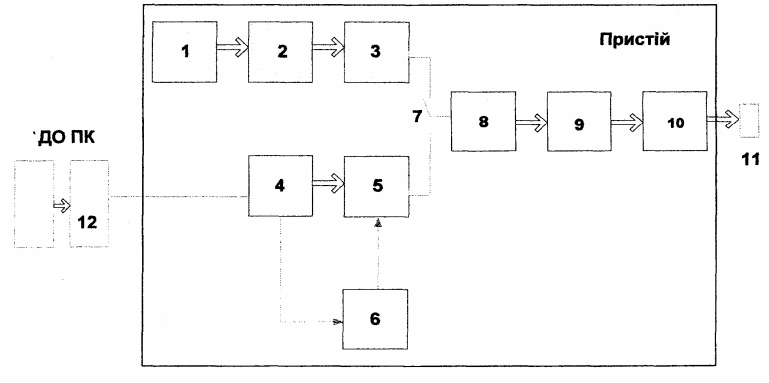
СИСТЕМА ЗАХИСТУ ТЕРИТОРІЙ ВІД ВПЛИВУ БІОЛОГІЧНИХ ОБ'ЄКТІВ

В. П. Марценюк, к.т.н., доцент
Вінницький національний технічний університет
walmar@ua.fm

Захист територій від впливу біологічних об'єктів, котрі можуть порушувати надійність роботи систем захисту периметрів від несанкціонованого доступу на практиці здійснюється шляхом використання ультразвукових електронних систем. Такі системи здатні формувати на території, що захищається, некомфортні чи навіть небезпечні для життя умови існування біологічних об'єктів впливу і змусити їх тим самим залишити периметр захисту. Ультразвукові системи випромінюють акустичні сигнали, діапазони частот яких є різними для різних видів біологічних об'єктів. Більшість з цих частот є ультразвуковими і вони повинні мати рівень випромінювання безпечний для людини. Цей рівень визначається ДСТУ 12.1.001-89 «Ультразвук. Загальні вимоги до безпеки».

Розглянемо принцип побудови структур електронних систем відлякування біологічних об′єктів на прикладі структури наведеної на рисунку. Генеруючим пристроєм такої системи служить персональний комп'ютер, здатний програмним шляхом організовувати періодичне формування звукових фрагментів страху конкретних біологічних об'єктів з виведенням цих фрагментів через послідовний COM-порт типу RS232. Передбачена періодична зміну спектрального складу ультразвукових коливань, що зменшує ефект звикання.

Система містить n - пристроїв відлякування кожен у складі генератора імпульсів 1, лічильника 2, блоку постійної пам'яті 3, інтерфейсу зв'язку 4, блоку оперативної пам'яті 5, схеми керування 6, перемикача режимів 7, цифро-аналогового перетворювача 8, аналогового фільтра 9, підсилювача потужності 10 і акустичної системи 11. У цій системі з метою підвищення гнучкості її використання додатково введена можливість автономної роботи підсистеми випромінювання. Для цього в склад структури системи введено додаткові елементи у вигляді блоку постійної пам’яті та перемикача режимів.



В режимі автономної роботи для формування сигналів відлякування використовуються фрагменти попередньо записані в постійній пам’яті пристрою. Ці фрагменти циклічно виводяться з цієї пам’яті за допомогою схеми управління на базі генератора та лічильника і подаються на цифро-аналоговий перетворювач для подальшого формування.

УДК 681.3.067

ЕЛАСТИЧНІСТЬ ЯК ФУНКЦІЯ ОЦІНКИ ВРАЗЛИВОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Ю. П. Гульчак, к.т.н., доцент
Ю. В. Бойко, асистент
Е. Ю. Гульчак, студент
Вінницький національний технічний університет
jurigulchak@rambler.ru

Узагальнена оцінка вразливості і захищеності інформаційних ресурсів підприємства є функцією від багатьох складових (видів загроз), кожна з яких вносить свою частину в підвищення чи пониження загального рівня безпеки.

У доповіді представлені структуровані загрози за основними напрямками захисту, такими як захист об'єктів інформаційної системи; захист процесів, процедур і програм обробки інформації; управління системою захисту.

Побудова математичної моделі передбачає формалізацію загроз і визначення функції відповідності між загрозами y_i та факторами їх виникнення x_i. В доповіді групи загроз поділені за ознаками:

- однозначної відповідності загрози y і фактора x, тобто спрощений випадок, коли $y=f(x)$;
- загроза у залежить від багатьох факторів x_i, тобто маємо функцію кількох аргументів $y=f(x_1,x_2,...x_к)$;
- один і той же фактор x_i впливає на рівень захищеності від багатьох загроз, тобто $y_1,y_2,...y_к=f(x)$;

- загрози та їх фактори пов'язані перехресними зв'язками, тобто $y_1,y_2,...y_к = f(x_1,x_2,...x_к)$.

При однозначній відповідності кількісно ступінь впливу окремо взятого фактора x на загрозу y можна оцінити за допомогою похідної, однак неоднорідність величин y та x не дозволяє отримати однозначну інформацію про загрозу як елемент захисту. Щоб врахувати прив'язаний до базового або середнього відносний рівень загроз за рахунок середнього деякого фактора в економіці існує поняття еластичності функції. З точки зору безпеки еластичність можна трактувати як відносну зміну (варіативність) загрози $y_к$ за рахунок відносної зміни фактора ризику x_i. Така оцінка дає можливість співставляти різнорозмірні величини y та x. Еластичність є логарифмічною мірою інформаційного ресурсу:

$$\varepsilon_x^y = \frac{\lim}{\Delta x \to 0}\left(\frac{\Delta y}{y} \Big/ \frac{\Delta x}{x}\right) = \frac{x}{y} y' , \quad \text{або} \quad \varepsilon_x^y = \frac{d \ln y}{d \ln x} .$$

Таке трактування дозволяє виявити подібність наведеного вище виразу до формули Шенона або Хартлі. Деякі автори щоб пов'язати їх вводять поняття доцільності інформації. Нас же цікавить кількість інформації як інформаційна ємність (місткість) окремого інформаційного ресурсу і зміна його первинної ємності за рахунок реалізації деякої загрози.

В роботі проаналізовані фактори несанкціонованого впливу на структуровані інформаційні ресурси (активи) підприємства на основі яких створена модель, яка дозволяє кількісно, не залучаючи експертні та статистичні оцінки, визначити ступінь надійності інформаційного активу за загрозами, викликаними факторами ризику, якщо рівень безпеки ІС понижується, а також ввести додаткові фактори захищеності для підсилення рівня безпеки до прийнятного.

УДК 003.26

МЕТОДИ ПОБУДОВИ ШВИДКИХ АЛГОРИТМІВ ХЕШУВАННЯ

Ю. В. Баришев, магістр з інформаційної безпеки, аспірант
Вінницький національний технічний університет
numen@svitonline.com

Відомо, що для хеш-функцій з теоретично доведеною стійкістю, їх стійкість або опір колізіям прямо пропорційний довжині значення. В той же час, чим більша розрядність хеш-значення, тим більше обчислень функції необхідно виконати для його визначення, а тому ці обчислення вимагають достатньо багато часу. Збільшення розрядності мікропроцесорів дозволяє виконувати такі обчислення швидше. Однак, з іншого боку, воно і дозволяє зловмиснику швидше "зламати" хеш-функцію, відповідно доводиться знову збільшувати розрядність хеш-значення. Таким чином, покращення апаратури не обумовлює, в загальному випадку, збільшення швидкості обчислення хеш-значення. Виходячи з цих міркувань, можна зробити висновок, що актуальною є задача побудови хеш-алгоритмів, які б дозволяли підвищити швидкість обчислень без втрати стійкості хеш-функції.

Розглядається хеш-функція теоретично доведеної стійкості, яка базується на операції піднесення до степеня за модулем простого числа. Для обчислення занчень таких хеш-функцій вхідні дані розбиваються на блоки $X = \{x_i\}$ ($i = 1 \div n$) і в кожному з раундів обчислюється значення функції:

$$y_i = f(x_i, y_{i-1}),\ y_0 = const\ . \qquad (1)$$

Відомо, що операція піднесення до степеня чисел великої розрядності вимагає достатньо багато машинного часу. Якщо ж суттєво зменшити розрядність числа, то піднесення до степеня буде виконуватись швидко, але це дозволить швидше "зламати" хе-функцію. Для того, щоб запобігти цьому, пропонується заміщувати одне рівняння з великою розрядністю системою рівнянь, а хеш-значення на кожному раунді отримувати шляхом конкатенації хеш-значень кожного *j*-го рівняння $y_i = \{y_{ij}\}$ ($j = 1 \div k$). Тоді вхідні дані X будуть розбиватись не n, а на $n \cdot k$ частин, а процес хешування можна розпаралелити, обчислюючи на кожному процесорі рівняння:

$$y_{ij} = f_j\left(x_i, y_{(i-1)j}\right). \qquad (2)$$

Проте вихідне хеш-значення, отримане шляхом конкатенації на останньому раунді всіх хеш-значень рівнянь $y_{(n\cdot k)1} \| y_{(n\cdot k)2} \| \ldots \| y_{(n\cdot k)k}$ буде не стійким до атаки Жоукса (Joux) та похідних від неї атак на хеш-функції. Тому пропонується з метою запобігання цих атак виконувати зав'язку на кожному *i*-му раунді кожного *j*-го хеш-значення, що отримується за допомогою *j*-го рівняння, та всіх хеш-значеннь, отриманих на попередньому $(i-1)$-му кроці. Таким чином, рівняння (2) буде заміщене таким рівнянням:

$$y_{ij} = f_j\left(x_i, y_{(i-1)1}, y_{(i-1)2}, \ldots, y_{(i-1)k}\right). \qquad (3)$$

А хеш-значення $y_{(n\cdot k)1} \| y_{(n\cdot k)2} \| \ldots \| y_{(n\cdot k)k}$ буде стійким до атак, похідних від атаки Жоукса, одночасно дозволяючи виконати розпаралелення обчислень.

УДК 003.26+511.17

ГЕНЕРУВАННЯ ПАР ВЗАЄМНО ПРОСТИХ ЧИСЕЛ

О. В. Дмитришин, магістр з інформаційної безпеки, аспірант
Вінницький національний технічний університет
olexanderdm@gmail.com

Для побудови сучасних симетричних блокових шифрів, які використовують операції множення за секретним змінним модулем, потрібні пари взаємно простих чисел. Відомі такі методи перевірки чисел на взаємну простоту, як алгоритм Евкліда і алгоритм ділення, які за своєю архітектурою не є швидкими. Все це зумовлює актуальність пошуку нових методів генерування пар взаємно простих чисел.

Відомим є таке твердження, що для будь-якого $a \in N$, число $(2a + 1)$ буде взаємно простим з a, тобто

$$\text{НСД}(a, 2a+1) = 1.$$

Вище згадане твердження використано для розроблення метода генерування пар взаємно простих чисел, основна ідея якого полягає в том, що генерують n-бітне псевдовипадкове число $p = \{x_0, x_1, \ldots, x_{n-1}\}$, де x_0 – найбільш значущий біт, а x_{n-1} – найменш значущий біт і $a = \{x_1, \ldots, x_{n-1}\}$. Тоді, генерування пар взаємно простих чисел a і b виконується за таким правилом:

$$a = \begin{cases} a = a + 1, \textit{якщо } x_0 = 0 \\ a = a - 1, \textit{якщо } x_0 = 1 \end{cases}, \quad b = \begin{cases} b = 2a - 2, \textit{якщо } x_0 = 0 \\ b = 2a - 1, \textit{якщо } x_0 = 1 \end{cases}.$$

Отже, для n-розрядного генератора псевдовипад-кових чисел використовуючи запропонований метод генерування пар взаємно простих чисел можна отримати 2^{n-1} таких пар.

УДК 378.381

ПСИХОЛОГІЧНІ АСПЕКТИ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

А. В. Дудатьєв, к.т.н., доцент
В. М. Дудатьєва, асистент
О. Д. Кец, студент
Вінницький національний технічний університет
dima.kec@gmail.com

Захист інформації розуміє під собою не лише використання відомих механізмів захисту але і кваліфіковані кадри. Відомий факт, що самою слабкою ланкою в цьому ланцюгу є людський фактор. Практично всі підприємства, заводи, корпорації вкладають великі кошти в апаратні засоби захисту інформації, в аналіз, моніторинг, розробку внутрішньої політики безпеки. І в останню чергу звертають увагу на психологічну підготовку спеціалістів, що в більшості випадків призводить до краху всієї системи захисту.

Психологічний вплив може бути як мінімум з двох сторін. В першу чергу із сторони компанії, а саме запровадження контролю щодо стимулювання виконання правил безпеки і певні міри покарання. З іншого боку, це зовнішній вплив на працівника сторонньої компанії. Для цього можуть використовуватися різні методи психологічної атаки, а саме: можливість заробити вкравши інформацію, можливість дезінформування співробітника з метою дізнатися секретну інформацію видаючи її як загальнодоступну. В доповіді розглянуті та запропоновані конкретні рекомендації та механізми щодо використання психологічних аспектів підготовки фахівців у галузі інформаційної безпеки.

У цілому, психологічне забезпечення комерційної таємниці в процесі відбору, підготовки, висування й звільнення кадрів ефективніше й дешевше, ніж при звичайному засекречуванні інформації.

Супровід персоналу є одним з невід'ємних елементів процесу забезпечення корпоративної безпеки кожної фірми й організації.

Моніторинг співробітників необхідний для відстеження змін, що відбуваються зі співробітником у процесі роботи на фірмі, у компанії, організації й появи в нього якостей, що породжують загрозу корпоративній безпеці.

У багатьох компаніях серйозна увага приділяється питанням корпоративного навчання. Таке навчання сприяє виробленню згуртованості, підвищенню працездатності команди, допомагає сформувати резерв на висування.

Поряд з обговоренням професійних питань, у ході навчання повинні розглядатися різні аспекти особистої й корпоративної безпеки.

Основними напрямками навчання можуть стати:

- правила роботи з документами, що містять комерційну таємницю;
- прийоми й методи, використовувані в промисловому шпигунстві;
- ефективна ділова комунікація;
- дії в екстремальних ситуаціях;
- тактика ведення переговорів і протидія маніпулятивному впливу;
- питання особистої безпеки при знаходженні за межами фірми.

3. МЕТОДИ ТА ЗАСОБИ УЩІЛЬНЕННЯ ІНФОРМАЦІЇ

УДК 681.3

СПОСІБ УЩІЛЬНЕННЯ ДАНИХ ПРИ ЇХ ПОДАННІ У ВИГЛЯДІ ДВОВИМІРНОГО ГРАФІЧНОГО КОДУ

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

За допомогою двовимірних графічних кодів можна подавати будь-які алфавітно-цифрові дані, що належать розширеному ASCII. Проте, при створенні певної множини алфавітно-цифрових повідомлень може використовуватись обмежений набір символів (алфавіт повідомлень). Якщо потужність такого алфавіту менша за 256 (потужність розширеного ASCII), з’являється можливість закодувати повідомлення так, що для двійкового значення кожного символу текста знадобиться менше, ніж 8 бітів. Тобто, з’являється можливість ущільнення даних. Актуальність даної задачі пов’язана з тим, що ущільненому повідомленню буде відповідати ГК-позначка меншої площі, завдяки чому можна мініатюризувати позначки або збільшити їх інформаційну ємність при незмінних геометричних розмірах.

При створенні ГК-позначок двовимірних двоколірних графічних кодів часто використовують бітове подання даних, а для забезпечення надійного зберігання графічно-кодованих даних використовують завадостійкий код Ріда-Соломона, який є многозначним кодом, тобто оперує з недвійковими символами. Мінімальними інформаційними одиницями (розрядами) для коду Ріда-Соломона є q-значні (q>2) символи – елементи поля Галуа GF(q). Щоб об’єднати можливість використання бітового

способу заповнення матриці даних графічного коду і потребу забезпечення завадостійкого захисту даних на основі коду Ріда-Соломона, використовують поле Галуа з розмірністю $q = 2^s$. Наприклад, при s=8 елементами поля будуть числа від 0 до 255, а операції над ними слід виконувати за модулем незвідного многочлена степеня 8.

Кодування алфавітно-цифрової послідовності, що використовує вхідний алфавіт потужності P_A, зводиться до перетворення символів вхідного алфавіту A в символи вихідного алфавіту Ω: $n(P_A) \to m(P_\Omega)$, тобто n символів алфавіту A перетворюють в m символів алфавіту Ω. Це можна реалізувати як перетворення n-розрядних чисел з системи числення за основою P_A в m-розрядні числа системи числення за основою P_Ω. Довжина n-розрядного числа в системі числення за основою P_A становить $n \cdot]\log_2 P_A[$ розрядів, а довжина m-розрядного числа в системі числення за основою P_Ω – $m \cdot]\log_2 P_\Omega[$ розрядів.

Таким чином, для ущільнення алфавітно-цифрових даних необхідно і достатньо, щоб виконувалась умова:

$$\begin{cases} P_A^n \le P_\Omega^m \\ n \cdot]\log_2 P_A[> m \cdot]\log_2 P_\Omega[\end{cases}.$$

Виконання даної умови при фіксованому P_Ω зводиться до знаходження P_A (потужності вхідного алфавіту), тобто до знаходження основи системи числення, при якій буде забезпечуватись ущільнення даних.

Наприклад, при P_Ω=256 ущільнення алфавітно-цифрових даних можливе, якщо використовувати алфавіт з потужністю 40 або 84, а цифрових даних – якщо вони подаються у 3-ковій, 5-ковій або 10-ковій формі.

УДК 621.038

СЖАТИЕ БИНАРНЫХ ИЗОБРАЖЕНИЙ НА ОСНОВЕ БИНОМИАЛЬНЫХ ЧИСЕЛ

И. А. Кулик, к.т.н., доцент
С. В. Костель, аспирант
Сумской государственный университет
eikt@ukr.net

Для того чтоб максимально упростить и ускорить решение задач, связанных с обработкой полутоновых (многоградационных) по яркости изображений, используют бинарные (двухградационные) изображения. При этом каждая бинарная сцена имеет только одно из двух значений яркости, условно обозначаемых через 0 и 1. Важно отметить, что изображения представляют собой особенный тип данных, обладающий значительной информационной избыточностью, и без специальной обработки они занимают большие объемы памяти. Поэтому задача сжатия бинарных изображений является актуальной.

В данной работе предлагается теоретическое описание метода сжатия бинарных изображений на основе биномиальных чисел. Метод основан на нумерации бинарных последовательностей при помощи биномиальных чисел.

Основой метода является использование биномиальной системы счисления, в которой в качестве оснований стоят биномиальные коэффициенты.

Алгоритм сжатия с использованием биномиальных чисел состоит из следующих операций:

1. Считывание двоичной последовательности определенной длины n из массива исходных данных;

2. Подсчет количества k единиц двоичной последовательности;
3. Преобразование двоичной кодовой комбинации в биномиальное число. Эта операция состоит в отбрасывании в двоичной комбинации единиц справа до первого появления нуля или отбрасывании нулей справа до первой единицы.
4. Переход от биномиального числа к его порядковому номеру в биномиальной системе счисления с параметрами n и k. Для нахождения порядкового номера используют кодообразующую функцию. Суть расчета состоит в нахождении значений биномиальных коэффициентов с определенными индексами и их последующем сложении.

Рассмотренный метод сжатия на основе биномиальных чисел весьма эффективен для сжатия бинарных изображений с преобладанием в них одного из цвета (черного или белого). Коэффициент сжатия зависит от размеров сжимаемых блоков n и распределения черных и белых пикселей в каждом из блоков. Чем больше отклонение распределения пикселей от среднего значения $n/2$, тем больше коэффициент сжатия. Следовательно, существует необходимость в предварительной оценке сжимаемого изображения с целью получения максимального коэффициента сжатия. При увеличении размера сжимаемого блока n, коэффициент сжатия также увеличивается. Возрастающие при этом временные и аппаратурные затраты, связанные с подсчетом биномиальных коэффициентов для больших значений n и k, можно уменьшить, если применять быстродействующие методы расчета биномиальных коэффициентов.

УДК 621.39

СТВОРЕННЯ ВЕКТОРНИХ КОДОВИХ КНИГ ДЛЯ УЩІЛЬНЕННЯ МОВИ

О. М. Ткаченко, к.т.н., доцент
О. Д. Феферман, аспірант; С. В. Хрущак, аспірант
Вінницький національний технічний університет
ant@vstu.vinnica.ua

Для ущільнення мовних сигналів часто застосовують методи на основі лінійного прогнозування. Але замість коефіцієнтів LPC на практиці застосовують еквівалентну форму їх представлення у вигляді лінійних спектральних пар (LSP).

Для подальшого 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. Одним з основних недоліків векторного квантування є те, що тривалість пошуку вектора у кодовій книзі досить висока і це заважає обробляти мовні сигнали в режимі реального часу.

Пропонується новий підхід до впорядкування векторів у кодовій книзі, що дозволяє досягти зменшення складності обчислень. Підхід базується на створенні структурованих векторних кодових книг. Кодова книга розбивається на класи, що не перекриваються між собою та містять різну кількість векторів. Кожен вхідний вектор також можна віднести до певного класу, при цьому пошук відповідного йому класу зводиться до простої процедури порівняння та не вимагає значних обчислювальних витрат.

Математична модель упорядкування векторів базується на відношенні мажорування. В загальному, мажорування дозволяє розмістити вектори у певній чіткій послідовності, але. для LSF побудова такої послідовності не завжди можлива. Тому ці вектори розбиваються на групи (рівні), а відношення мажорування застосовується не до самих векторів а до створених рівнів. Ця операція називається структуризацією векторних кодових книг. Структуризація має на меті скорочення обчислювальних витрат на пошук квантованого вектора у кодовій книзі, що є найближчим до вхідного вектора.

Структуровані кодові книги будуються для кожного підвектора незалежно. Основна ідея методу прискореного пошуку полягає у тому, що найближчі до вхідного вектора квантовані вектори в кодовій книзі мають знаходитися на тому ж рівні мажоризації, що і вхідний вектор, або на сусідніх рівнях. За рахунок цього з'являється можливість значно скоротити число кандидатів на відбір і, відповідно, зменшити час пошуку.

Пошук найближчого вектора відбувається в два етапи. На першому етапі відбувається пошук рівня мажоризації, якому належить вхідний вектор. Перевірка відношення мажорування потребує набагато менше обчислювальних витрат порівняно з обчисленням відстані. Далі відбувається пошук найближчого до вхідного квантованого вектора на знайденому рівні мажоризації та кількох сусідніх рівнях.

Результати проведених досліджень показали що структурування кодових книг дозволяє зменшити обчислювальну складність та збільшити швидкість пошуку в кодовій книзі.

УДК 621.39

ВИКОРИСТАННЯ МЕТОДУ ДЕЛЬТА УЩІЛЬНЕННЯ ДЛЯ ВОКОДЕРА MELP

О. М. Ткаченко[1], к.т.н., доцент
О. Д. Феферман, аспірант; С. В. Хрущак[2], аспірант
Вінницький національний технічний університет
[1]ant@vstu.vinnica.ua, [2]sergey.khruschak@gmail.com

Найбільш ефективними методами ущільнення мовлення є параметричні методи ущільнення, які оперують не з вихідним мовленнєвим сигналом, а його параметрами, обчисленими на кадрі. Більшість систем параметричного ущільнення мовленнєвого сигналу засновано на моделі лінійного прогнозування із незалежним функціонуванням джерела збудження звукової хвилі в мовотворному тракті та власне артикулярного акустичного фільтра – кодування з лінійним прогнозуванням (LPC).

Основний развиток вокодерів за останні роки відбувався у напрямку удосконалення механізму формування джерела збудження. Покращення якості вокодерів йшло шляхом використання багатоімпульсного збудження та використання векторних кодових книг, отриманих в результаті кластеризації коефіцієнтів, що описують мовленнєвий тракт.

Одним з таких вокодерів є вокодер MELP, який забезпечує гарну якість сигналу на бітовій швидкості 4 кБіт/с. Для подальшого зменшення бітової швидкості, при забезпеченні природньої якості сигналу пропонується для опису артикулярного акустичного фільтра використовувати метод дельта ущільнення з прогнозуванням. Даний метод заснований на використанні впорядкованих кодових книг та дозволяє враховувати

кореляцію між сусідніми наборами коефіцієнтів для опису спектральної складової сигналу. Впорядкування кодової книги відбувається за методом мажорування.

Суть даного методу полягає в тому, що замість векторів кодової книги передається прогноз різниці між сусідніми векторами. Прогноз різниці між значеннями індексів векторів лежить в межах заданого вікна, яке є значно меншим за розмір самої кодової книги. Це дозволяє передавати на приймальну сторону меншу кількість бітів для опису вектора в кодовій книзі і таким чином отримати додаткове ущільнення. Прогнозування відбувається шляхом створення екстраполюючої функції для індексів кількох кадрів на приймальній та передавальній стороні. Для прогнозу різниці використовується метод найменших квадратів.

Для зменшення спотворення, що вноситься в сигнал за рахунок дельта-ущільнення введено додаткову затримку сигналу в 1 кадр. Введення затримки дозволяє корегувати значення дельти, які передаються, що необхідно в ситуаціях, коли прогноз виявляється невірним. Корекція прогнозу відбувається на основі апроксимації отриманих індексів кодової книги та полягає у внесенні похибки в прогноз поточного значення для мінімізації сумарної похибки для поточного та наступного значень.

Результати проведених досліджень показали що використання методу дельта-ущільнення з прогнозуванням у вокодері MELP дозволяє зменшити бітову швидкість, необхідну для передачі мовленнєвого сигналу, при незначній втраті якості синтезованого мовлення.

УДК 004.2:004.93:654.915:681.3

РОЗРОБКА ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ УЩІЛЬНЕННЯ ТА РОЗПІЗНАВАННЯ ПЛЯМОВИХ ЗОБРАЖЕНЬ

А. А. Яровий, к.т.н., доцент; Р. С. Власюк, студент
Вінницький національний технічний університет

Часова природа лазерного променя дозволяє йому змінюватися від нескінченої хвилі до надзвичайно короткого імпульсу. Когерентність лазеру дозволяє йому переміщуватися по вузькому променю, з маленькою і визначеною дивергенцією. Це дозволяє користувачу точно визначити ділянку, яка освітлюється лазерним променем. Саме завдяки когерентності лазерний промінь може бути сфокусований в дуже маленьку насичену пляму на високо-концентрованій ділянці. Ця сконцентрованість робить лазерний промінь корисним для застосування у фізиці, хімії, медичній індустрії та в промислових застосуваннях. Тому актуальним є дослідження процесів формування профілю променя, який знаходиться в процесі розвитку, у відповідності з яким інтенсивність лазерного променя змінюється вздовж поперечного перерізу.

В роботі розроблено інтелектуальну систему (ІС) ущільнення та розпізнавання плямових зображень (128x128 пікселів) лазерного променя, що у своїй сукупності формують його профіль. Основна увага приділяється динамічній обробці та розпізнаванню плямових зображень відео-траси лазерного променя в реальному часі, що в свою чергу призводить до необхідності попередньої обробки із одночасним ущільненням зображень для подальшого їх динамічного розпізнавання за допомогою нейронної мережі (на основі персептронних структур).

В ході проведених досліджень здійснено імітаційне моделювання (14 відео-трас по 2044 плямових зображення) та програмну реалізацію ІС ущільнення та розпізнавання плямових зображень. В системі використовуються вхідні плямові зображення протяжної лазерної траси в кольоровій моделі RGB, а оброблення зображення виконується посередництвом використання певних компонент моделі CIE XYZ. Без процедури ущільнення для опису початкового вхідного зображення заданої розмірності необхідно було б: 128x128x3=49152 байт пам'яті, що суттєво знижує ефективність обробки при подальшому поданні на входи нейромережевої структури. Тому в системі застосовується сегментація (топологічний аналіз) зображення з подальшим усередненням кольору сегменту. На основі експериментальних досліджень області на зображенні було класифіковано за впливом на розташування „енергетичного центру" та загальною оцінкою „правильності" плями. Кожне зображення розбивається на 5 кілець інтенсивності та відповідно на 30 зон, що в свою чергу обумовлює суттєве підвищення ефективності обробки при подальшому поданні на входи нейромережевої структури.

Результати нейромережевого розпізнавання зображень

Параметр	**+**	**-**	**all**	**Параметр**	**+**	**-**	**all**
Вибірка 1	20	20	40	Вибірка 2	100	100	200
Розпізнано	17	19	36	Розпізнано	92	87	179
У відсотках	85	95	90	У відсотках	92	87	89,5

де „+" – клас правильних зображень (хороші), „- " – клас спотворених зображень (погані), „all" – всього зображень.

Тестування ІС по всій довжині траси (2044 зображення) в реальному часі показало результати, відповідно: 74% коректно класифікованих "хороших" зображень та 60% - "поганих". Результати тестування свідчать про працездатність та адекватність обраного підходу.

УДК621.382

ЗМЕНШЕННЯ НАДЛИШКОВОСТІ ІНФОПОТОКІВ В ІНФОРМАЦІЙНИХ СИСТЕМАХ.

Ю. Ю. Іляш, аспірант
Прикарпатський національний університет
імені Василя Стефаника, м. Івано-Франківськ,
yurchukil@gmail.com

В інформаційних системах залежно від типу інформації (голосове повідомлення, фото- чи телезображення, послідовність чисел, сигнали контролю і управління …) формуються інформаційні потоки різного характеру,. У відповідності до характеру джерела інформації та його статистичних характеристик визначають методи та засоби математичного представлення інфопотоків. В залежності від типу даних, що обробляють, визначають ефективні методи зменшення надлишковості, які орієнтовані на відповідні інфопотоки.

Для визначення ефективності методів зменшення надлишковості інфопотоків доцільнішим є обчислення коефіцієнта зменшення надлишковості за числом двійкових одиниць, оскільки він враховує службову інформацію необхідну для відновлення сигналу.

Для знаходження коефіцієнта за двійковими значеннями необхідно визначити об’єми сформованих повідомлень:

— об’єм без зменшення надлишковості

$$V_1=n*\text{roundup}[\log_2 A]; \quad (1)$$

— об’єм в звичайних адаптивних системах зменшення надлишковості

$$V_2=n'*(\text{roundup}[\log_2 A] + \text{roundup}[\log_2 n]), \quad (2)$$

де A – кількість рівнів квантування, roundup[ ] – функція округлення до більшого цілого.

Користуючись рекурсивними кодовими послідовностями Галуа кожну мітку часу можна передати одним бітом, завдяки чому зменшити об'єм службової інформації у тих випадках, коли кількість істотних відліків становить $\left(\frac{n}{\text{roundup}[\log_2 n]}\right)/n \cdot 100\%$ від загальної кількості відліків. У цьому випадку об'єми формованих повідомлень можна обчислити за формулою [3]:

$$V_3 = n' * (\text{roundup}[\log_2 A]+1)+(n-n') =$$
$$= n' * \text{roundup}[\log_2 A]+n \qquad (3)$$

Для дослідження ефективності адаптивних систем зменшення надлишковості інфопотоків використано вимірювальні сигнали двох типів: пилоподібний та прямокутної форми, які використовуються в телеметричних системах.

Таким чином, проведено аналіз відомих адаптивних систем зменшення надлишковості інфопотоків. Наведено результати аналізу методів передбачення нульового порядку при застосуванні до сигналів прямокутної та пилоподібної форми. Досліджено адаптивну систему зменшення надлишковості інфопотоків із часовою прив'язкою істотних відліків рекурсивними кодовими послідовностями Галуа до часу появи їх дискретів. Виявлено, що перевагою досліджуваної системи є формування менших об'ємів формованих потоків даних. Спосіб формування службової інформації, яка вноситься в оброблюваний інфопотік, дозволяє отримати високі коефіцієнти зменшення надлишковості. Недоліком системи є формування службової інформації більших об'ємів при малому відношенні кількості істотних відліків до загальної кількості відліків.

УДК 681.32

УЩІЛЬНЕННЯ ДАНИХ НА ОСНОВІ КЛАСТЕРНОГО АНАЛІЗУ

В. П. Семеренко, к.т.н., доцент
О. О. Сухоносов, магістрант
Вінницький національний технічний університет
VPSemerenko@mail.ru

В останні роки все більше розповсюдження отримує нова парадигма обробки даних, коли замість ущільнення і збереження всіх даних, зберігається лише отримана із початкових даних корисна інформація, тобто, знання. Для здобування знань розроблено різноманітні методи інтелектуального аналізу даних (Data Mining), зокрема, кластеризація – розподіл множини всіх об'єктів на групи "схожих" об'єктів. Під час групування однорідних об'єктів їх можна об'єднувати по заданим критеріям виконуючи тим самим і задачу ущільнення даних.

Перші алгоритми кластеризації були орієнтовані на ідеалізовану модель, в якій кожний об'єкт міг належати тільки одному кластеру. Більш практичним є підхід, який враховує взаємозв'язок між об'єктами, а не взаємозв'язок між об'єктом і центром кластеризації, якого в загальному випадку може і не бути. Такий підхід може бути отримано на основі представлення кластерів нечіткими множинами і припущенні, що один об'єкт може належати кільком кластерам з різним ступенем приналежності. Це буде можливим, якщо границі сусідніх кластерів розмиті. Оскільки неможливо точно визначити границі кластерів, то, відповідно, неможливо точно визначити і форму функцій приналежності (ФП) об'єктів кластерам. Таким чином, і самі ФП повинні бути нечіткими.

Саме тому найбільш придатним математичним апаратом для опису взаємозв'язку таких об'єктів може бути нечітка логіка вищих порядків (Типу 2).

Для заданої довільної непустої множини елементів (об'єктів) X з n атрибутами використовується інтервальна нечітка Типу 2 підмножина

$$\widetilde{A} = \{((x,u), \mu_A(x,u)) \mid x \in X, u \in \int_x \subseteq [0,1]\},$$

$$x \in X,\ \mu_A(x,u) \in [0,1]$$

де $\mu_A(x,u) \in \{0,1\}$ є інтервальною Типу 2 ФП нечіткої підмножини $\widetilde{A}$(первинна ФП), а $\int_x -$ область ФП множини X (вторинна ФП).

Метод кластеризації на основі нечіткої логіки Типу 2 є агломеративним і, на відміну від відомих методів Fuzzy C-Means та Гюстафсона-Кесселя, не вимагає задання центрів кластерів і не обмежує форму кластера еліпсоїдом. На i-й ітерації в кластер об'єднуються об'єкти, які розташовані на відстані по заданим атрибутам d_j $(j = 1 \div n)$. При формуванні нових кластерів використовуються операції об'єднання і перетину нечітких ФП.

Вибрані на i-й ітерації об'єкти одного кластера усереднюються по всім атрибутам і замінюються узагальненим об'єктом. На $(i+1)$-й ітерації в кластер об'єднуються початкові та узагальнені об'єкти, тобто на кожній ітерації загальна кількість об'єктів зменшується. Критерієм закінчення процесу ущільнення може бути досягнення граничної величини відстані d_j між об'єктами, або кількість об'єктів, що залишилась.

УДК 681.32

ПЕРЕТВОРЕННЯ ПРИ УЩІЛЬНЕННІ БЕЗ ВТРАТ

В. П. Майданюк, к.т.н., доцент
Вінницький національний технічний університет
maydan2000@mail.ru

Мета використання перетворень в ущільненні даних - перетворення одних видів надмірності в інші, простіше модельовані. Тобто, перетворення дозволяє представляти оброблювану інформацію в особливій формі, ідеально відповідній для подальшого ефективного кодування.

До таких перетворень відносять перетворення MTF (Move To Front) та перетворення BWT (Burrows-Wheeler Transform). Однак, якщо MTF давно використовується при ущільненні як в якості перетворення так і в якості самостійного методу ущільнення, то по-перше перетворення BWT може використовуватись тільки в якості перетворення, а по-друге за рахунок використання перетворення BWT сумісно з MTF можна досягнути значних коефіцієнтів ущільнення.

Моделювання показало, що застосування послідовно перетворення BWT, MTF та кодування серій нулів до повідомлень з невеликим алфавітом забезпечує кращі коефіцієнти ущільнення у порівнянні навіть з архіватором RAR. Так для повідомлень з алфавітом у чотири знаки коефіцієнт ущільнення у два рази вищий, а для повідомлень з алфавітом у вісім знаків у півтора рази. Однак, для стандартних текстових файлів коефіцієнт ущільнення значно нижчий. Причому, застосування архіватора до початкового файлу дає вищий коефіцієнт ущільнення у порівнянні з застосуванням його до файлу, отриманого після виконання ланцюжка перетворень.

УДК 681.3

УЩІЛЬНЕННЯ ДАНИХ ПРИ КЛАСИФІКАЦІЇ ЗА ДИСКРИМІНАНТНИМИ ФУНКЦІЯМИ

Т. Б. Мартинюк, к.т.н., доцент
А. В. Кожем'яко, к.т.н., доцент
О. М. Гуцол, магістрант; Ю. О. Панасюк, студент
Вінницький національний технічний університет
gotmog666@inbox.ru

Одним з прикладів використання дискримінантних функцій є класифікація біоелектричних сигналів (БЕС) в процесі біомедичної діагностики. Так відомий приклад розпізнавання БЕС за частотними ознаками спектрального аналізу вхідних даних, а саме, за значеннями смуги частоти Δf на заданому рівні і частоти максимуму спектра f_m.

В даній роботі пропонується метод, в якому використовується система дискримінантних функцій $g_i(Z)$, $i=\overline{1,m}$, де Z - вхідний образ, m - кількість класів класифікації C ($C=[C_1,\ldots,C_m]$). В даному методі приналежність вхідного образу до певного класу визначається за максимумом дискримінантної функції $g(Z)$ в системі дискримінантних функцій $g_i(Z)$

$$\begin{cases} g_1(Z)=w_{11}z_1+w_{12}z_2+\ldots+w_{1n}z_n \\ g_2(Z)=w_{21}z_1+w_{22}z_2+\ldots+w_{2n}z_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ g_L(Z)=w_{L1}z_1+w_{L2}z_2+\ldots+w_{mn}z_n, \end{cases} \qquad (1)$$

де w_{ij} - ваги, $i=\overline{1,m}$; $j=\overline{1,n}$.

Даний спосіб класифікації сигналів за дискримінантними функціями має всі ознаки нейромережної обробки векторних данних.

Використання обробки даних за різницевими зрізами дозволяє відмовитись від накопичення дискримінантних функцій $g_i(Z)$, вигляду (1).

Вхідними даними є вектор підмножини ознак образу $Z = \{z_1, \ldots, z_n\}$, матриця ваг $W = \begin{bmatrix} w_{11} & w_{12} & \ldots & w_{1n} \\ \ldots & \ldots & \ldots & \ldots \\ w_{m1} & w_{m2} & \ldots & w_{mn} \end{bmatrix}$. В результаті перемноження вхідних елементів та відповідних ваг, формуються значення елементів дискримінантних функцій $g_i(Z)$, які в подальшому зменшуються на загальну компоненту. Такі дії на вилучення найменших дискримінантних функцій повторюються доти, доки не залишиться остання дискримінантна функція, яка являється максимальною серед всіх, що дозволяє віднести об'єкт (Z), що розпізнається, до відповідного класу C_{i0}, $(i = \overline{1, m})$.

Таким чином, із вхідного вектора $Z = \{z_1, \ldots, z_n\}$ та матриці W формується матриця A^0 значень елементів дискримінант них функцій. В подальшому виконується обробка матриці A^0 з формуванням результуючого вектора Y, в якому одиничне значення приймає і-й елемент, що відповідає і-му класу.

Отже, в цьому випадку перехід від матриці елементів дискримінантних функцій розмірністю mxn до m-вимірного вектора класифікаційних ознак можна розглядати як варіант ущільнення даних, що має свої аналоги у нейромережних технологіях, наприклад, у картах Кохонена, що само організовуються (SOFM).

УДК 681.39

МЕТОДИ ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ ДЛЯ ПІДВИЩЕННЯ КОЕФІЦІЄНТА УЩІЛЬНЕННЯ

В. А. Каплун старший викладач
О. В. Михалевич, студент
Вінницький національний технічний університет
valuka@rambler.ru

Дана робота присвячена одному з підходів щодо ущільнення даних, який базується на представленні вхідного повідомлення у вигляді послідовності додатних цілих чисел, а вихідного повідомлення – у вигляді сукупності значень, отриманих методами, основою яких є обчислення відхилень, і певної додаткової інформації, необхідної для відновлення інформації без втрат. В результаті здійснених комп'ютерних досліджень було показано, що кожен із запропонованих методів забезпечує ефективне ущільнення тільки у разі певних властивостей вхідної послідовності цілих чисел. Тобто вибір конкретного методу повинен здійснюватись, виходячи саме з цих умов. І тому може бути використана додаткова процедура перетворення первинної послідовності до послідовності, яка матиме властивості, що задовольнять конкретному методу ущільнення.

Отже, степінь ущільнення інформації залежить від закону розподілу, якому відповідає вхідний потік початкової інформації. У доповіді пропонується декілька підходів до моделювання вхідного потоку даних.

Один з таких підходів полягає в тому, щоб ущільнювати не безпосередньо послідовність чисел вхідного повідомлення, а послідовність сум цих чисел, згрупованих певним чином. Адже доведено, що закон

розподілу отриманого ряду чисел наближений до нормального, і в цьому випадку деякі з запропонованих методів ущільнення, що базуються на обчисленні відхилень, можуть показати себе досить ефективними, оскільки розмір вхідної послідовності може виявитись набагато меншим, так само, як і значення відхилень .

Іншим підходом до моделювання даних може бути введення ваг розрядів чисел вхідної послідовності (наприклад, степені основи деякої системи числення), що може забезпечити значне зменшення обсягу ущільнених даних. Крім того, пропонується ще такий підхід, при якому вхідна послідовність заміняється на певним чином відфільтровану (наприклад, для ущільнення пропонується послідовність середніх значень за модулем чисел вхідної послідовності).

У кожному з запропонованих підходів до моделювання вхідних даних необхідно зберігати деяку додаткову інформацію для здійснення зворотного перетворення. Але це може компенсуватися тим, що значення відхилень, отриманих шляхом застосування запропонованих методів ущільнення, стануть досить малими, а отже, степінь ущільнення при цьому може значно зрости.

УДК 681.39

ДОСЛІДЖЕННЯ УМОВ МОЖЛИВОСТІ УЩІЛЬНЕННЯ МЕТОДАМИ, ЩО БАЗУЮТЬСЯ НА ОБЧИСЛЕННІ ВІДХИЛЕНЬ

В. А. Каплун, старший викладач
Т. М. Алєксєєва, студент
Вінницький національний технічний університет
valuka@rambler.ru

У зв'язку з тим, що сучасні мікропроцесори ефективніше здійснюють арифметичні операції над числами, для здійснення ущільнення запропоновано ряд методів, заснованих на представленні вхідних даних у вигляді послідовності цілих чисел, а ущільнені дані складаються з сукупності відхилень, отриманих певним чином. Серед цих методів такі, як: обчислення відхилень від сусіднього елементу вхідної послідовності, від констант, обраних певним чином; обчислення відхилень від центрів або середніх значень піддіапазонів, на які можна розбити діапазон представлення чисел заданої розрядності; обчислення відхилень від мінімальних, максимальних або середніх значень у групах, утворених при розділенні певним чином чисел вхідної послідовності на групи.

Звичайно, при використанні вказаних методів кожне з чисел ущільненої послідовності саме по собі буде мати меншу розрядність, аніж числа вхідної послідовності. Але для того, щоб можна було без втрат відновити інформацію після проведення ущільнення, необхідно зберігати ще й деяку додаткову інформацію: знаки відхилень, кількості відкинутих розрядів, ознаки констант, номери піддіапазонів, мінімальні, максимальні або середні значення тощо,

а залежно від того, який з методів використано в тому або іншому випадку.

У доповіді розглядаються результати проведених досліджень, для яких було відібрано ряд файлів різних форматів і різного обсягу. Для аналізу файли з вхідними повідомленнями представлялися у вигляді послідовностей чисел різної розрядності (від 8 до 2048). Для ущільнення методами, основою яких було розбиття на групи або піддіапазони, їх кількість варіювалася у досить широкому діапазоні для кожної з вибраних розмінностей. Результати аналізу показали, що обсяг ущільненої послідовності значною мірою залежить і від формату файлів вхідних повідомлень, і від розрядності чисел вхідної послідовності, і від кількості констант, груп або піддіапазонів, які приймали участь в обчисленні.

У роботі наведено теоретичні умови можливості ущільнення і показано, що для запропонованих методів найбільший коефіцієнт ущільнення досягається, коли значення чисел вхідної послідовності розподілені за нормальним законом. Але реальні послідовності можуть відповідати і іншим законам розподілу значень. Тому для досягнення найбільшого коефіцієнта ущільнення потрібно відповідним чином здійснювати перетворення вхідної послідовності чисел.

УДК 681.3

ЧИСЛОВІ МОДЕЛІ ДЖЕРЕЛА ДАНИХ, ЩО УЩІЛЬНЮЮТЬСЯ

Л. А. Савицька, асистент
Вінницький національний технічний університет

У відомих методах і алгоритмах ущільнення дані, в основному, розглядаються як набори або окремих символів, або сукупності символів, тобто слів. Практична реалізація таких методів є достатньо складною через те, що сучасні мікропроцесори орієнтовані на обробку чисел, а ні символів.

У доповіді розглядається підхід до ущільнення даних, який враховує особливості оброблення даних у сучасних мікропроцесорах. Суть підходу полягає в тому, що в процесі ущільнення будь-яка інформація розглядається як ціле додатне число.

Вихідні дані, що підлягають ущільненню, в мікропроцесорі представляються як послідовність символів 0 і 1. Відповідно до числової моделі джерела даних, послідовність символів розбивається на блоки, що містять деяку кількість символів (код), і кожному символу в блоці відповідає свій певний числовий еквівалент (вага розряду).

Відомо, що однозначність відображень коду в число і числа в код забезпечується умовою:

$$w_i > \sum_{j=0}^{i-1} w_j ; w_0 = 1,$$

де w_i - вага i-го розряду.

Виходячи з цього, для забезпечення великої кількості

можливих моделей джерела даних, пропонується обчислювати ваги розрядів коду за формулою:

$$w_i = \sum_{j=0}^{i-1} w_j + m; \quad w_0 = 1; \; w_1 = k; \; m = 1,2,...; \; k = 1,2,...$$

Таким чином, є можливість формувати послідовності чисел для вихідних даних, використовуючи $m \cdot k$ різних правил.

Наприклад, якщо вага *i*-го символу блоку дорівнює 2^i (*i*=0,1..., *n*-1), то блок є двійковим кодом числа, що обчислюється за формулою:

$$N = \sum_{i=0}^{n-1} a_i 2^i ,$$

де $a_i = \{0;1\}$.

Змінюючи кількість символів у блоці, будемо одержувати послідовності чисел з різними законами їхнього формування. Тобто для різних *n* будемо мати різні моделі джерела даних.

Модель джерела даних можна змінювати, змінюючи не тільки розрядність блоку, але й змінюючи за певним правилом символи в блоці.

Для простоти реалізації пропонується записувати в самий старший розряд блоку символ 1, якщо цей розряд містить 0. Тобто блок вигляду 0xx...x заміняється на блок вигляду 1xx...x, де x означає будь-який символ (1 або 0).

Можливість зміни моделі джерела даних дозволяє вибирати таку модель, що забезпечує найбільший коефіцієнт ущільнення для заданого правила кодування. Це є основою методів адаптивного ущільнення даних.

УДК 681.3

МЕТОД УЩІЛЬНЕННЯ ДАНИХ З РОЗБИТТЯМ НА БЛОКИ РІЗНОЇ ДОВЖИНИ

Шахзада Ашрафул Хок, аспірант
Є. А. Горобей, магістрант
Вінницький національний технічний університет

Існуючі методи й алгоритми ущільнення даних, в основному, враховують статистику символів у повідомленні або базуються на побудові словника. І хоча на практиці широко використовуються архіватори, створені на основі саме цих методів, пошуки нових підходів до ущільнення даних продовжуються.

Одним із цікавих підходів є пропозиція використовувати для ущільнення даних оптимізуючі властивості чисел Фібоначчі. Суть підходу полягає в тому, що в процесі ущільнення інформації блок цифрових даних будь-якої довжини розглядається як надвелике ціле додатне число, що представляється набором із трьох невеликих чисел. Таке представлення чисел, називається лінійною формою Фібоначчі.

Дослідження проведені авторами показали, що для фіксованої довжини блоків даних існують числа, які добре ущільнюються і які погано ущільнюються. Виходячи з цього, пропонується метод адаптивного ущільнення даних, суть якого така.

У лінійній формі Фібоначчі представляються числа, що відповідають блокам довжини від $l_{\min} = 2^a$ до $l_{\max} = 2^a + g \cdot 2^b$ з дискретністю 2^b. Тобто блоки мають такі довжини:

$$2^a, \left(2^a + 2^b\right), \left(2^a + 2 \cdot 2^b\right), \ldots, \left(2^a + g \cdot 2^b\right)$$

Значення a вибирається виходячи з мінімально припустимого коефіцієнта ущільнення. Значення b повинне задовольняти умові $b \le a$. Чим менше значення b, тим менше дискретність довжини й тим більше коефіцієнт ущільнення може бути отриманий. Але при цьому буде значно збільшуватися час ущільнення.

Серед усіх форм вибирається форма, що забезпечує найбільший коефіцієнт ущільнення ($S_{\text{ущ.}}$). Тобто реалізується така функція оптимізації:

$$f_{\text{бл}} = \max\left\{S_{\text{ущ}0}, S_{\text{ущ}1}, \ldots, S_{\text{ущ}g}\right\},$$

де $S_{\text{ущ}i}$ - коефіцієнт ущільнення i-го блоку даних, i=0,1,..., g.

Коефіцієнт ущільнення обчислюється за формулою:

$$S_{\text{ущ}\,i} = \frac{l_{\text{бл}\,i}}{l_{\text{S}i}},$$

де $l_{\text{бл}\,i}$ - довжина i-го блоку вихідних даних;

$$l_{\text{бл}\,i} = 2^a + i \cdot 2^b;$$

$l_{\text{S}\,i}$ - довжина блоку ущільнених даних.

Після того як визначено блок даних Блi, для якого одержано найбільший коефіцієнт ущільнення, цей блок видаляється з послідовності даних, що ущільнюються, і до частини, яка залишилася, застосовуються описані дії й визначається блок Блj, лінійна форма якого забезпечує найбільший коефіцієнт ущільнення. При цьому довжина блоку Блj може відрізнятися від довжини блоку Блi. Отже, довжина блоків, на які буде розбиватися послідовність даних, що ущільнюються, буде різною й адаптованою до найбільшого коефіцієнта ущільнення.

4. МЕТОДИ ТА ЗАСОБИ ПЕРЕТВОРЕННЯ ФОРМ ІНФОРМАЦІЇ

УДК 621.317.39

НОВІ МЕТОДИ ТА ЗАСОБИ ПЕРЕТВОРЕННЯ ФОРМ ВИМІРЮВАЛЬНОЇ ІНФОРМАЦІЇ

Ю. В. Шабатура[1], д.т.н., доцент
Ю.В. Бугайов[2]
[1]Вінницький національний технічний університет,
[2]ТОВ "ІВП ІнноВіннпром"
[1]shabatura@vntu.edu.ua
[2]Yurii.Buhaiov@innovinnprom.com.

Сучасні інформаційно-вимірювальні системи (ІВС) здатні вирішувати ряд важливих задач на основі тієї вимірювальної інформації, яку вони отримують з власних вимірювальних каналів. Незважаючи на велику різноманітність фізичних величин за їх природою, видом енергії носія, характером прояву і т.д., для вимірювання їх значень в ІВС як правило використовують методи і засоби електричних вимірювань фізичних величин. Практично це означає, що, якщо на вході вимірювального каналу сприймається сигнал фізичної величини будь-якої природи, то на його виході формується електричний сигнал, який є носієм вимірювальної інформації про значення вимірюваної фізичної величини. Традиційною формою представлення вимірювальної інформації є зміна одного, або кількох параметрів електричного сигналу. У якості таких параметрів використовуються амплітудні значення напруги, струму або заряду, частоту і фазу. Отже процедура вимірювань значень фізичних величин в такому разі зводиться до вимірювання відзначених параметрів електричних сигналів. При цьому показники якості вимірювання значень фізичних величин в значній мірі залежатимуть від метрологічних характеристик вимірювань відповідних параметрів електричних сигналів.

В доповіді пропонується розглянути використання для представлення вимірювальної інформації зміни часової тривалості електричних імпульсів і зміни довжини огинаючої імпульсів спеціальної форми. Запропоновані підходи передбачають розроблення нових методів і засобів для виконання процедур перетворення значень вимірюваних фізичних величин у зміни відзначених параметрів електричних імпульсів (перетворення форми вимірювальної інформації), а також відповідних методів і засобів для проведення якісних вимірювань таких параметрів.

Використання часової форми представлення вимірювальної інформації про значення фізичних величин дозволяє в комплексі вирішити задачу суттєвого підвищення точності вимірювань, а за рахунок переходу в імпульсний режим роботи підвищується завадостійкість вимірювань і зменшується енергоспоживання. Застосування мікросхем часо-цифрового перетворення дозволяє здійснювати вимірювання часової тривалості електричних імпульсів з роздільною здатністю біля 10 пікосекунд, що завдяки лінійності вимірювального перетворення трансформується в адекватний порядок точності вимірювань значень інших фізичних величин. Причому такі вимірювання можуть виконуватися в режимі одиночного імпульсу.

Використання зміни довжини огинаючої електричного імпульсу для представлення значення вимірювальних фізичних величин дозволяє враховувати комплексний характер окремих видів фізичних величин. Проведені дослідження дозволили з'ясувати оптимальні форми імпульсних сигналів для використання у вимірювальних перетвореннях з часовим представленням вимірювальної інформації і з представленням через зміну довжини огинаючої.

УДК 621.3.049

ЗАПАМ'ЯТОВУЮЧИЙ ПРИСТРІЙ НА БАЗІ АМОРФНИХ НАПІВПРОВІДНИКІВ

В. М. Кичак, д.т.н., професор
Н. Г. Курилова, аспірант; І. В. Слободян, студент
Вінницький національний технічний університет
sprtp@ukr.net

В теперішній час знаходять широке розповсюдження запам'ятовуючі пристрої (ЗП) на МДН структурах, перевагою яких є можливість збереження інформації при від-ключенні джерела живлення. На базі таких структур створюють ЗП, які допускають багаторазове перезаписування і зберігання інформації при відключеному живленні. Найбільш розповсюдженою на сьогодні є так звана флеш-пам'ять на базі МДН транзистора з двома ізольованими заслонами, один з яких є керуючим, інший – плаваючим. Основним недоліком такого виду пам'яті є обмежене число циклів перезапису. Ці недоліки обумовлені тим, що перезапис йде через стирання інформації, яке призводить до зносу мікросхеми. Тобто цей вид пам'яті не може замінити існуючі оптичні та магнітні ЗП через ненадійність і недовговічність. Це пов'язано з тим, що флеш пам'ять побудована на властивостях польових транзисторів зберігати електричний заряд в плаваючому заслоні. Наявність або відсутність заряду в транзисторі розглядається як логічний нуль або логічна одиниця. Для запису і стирання інформації використовується тунелювання електронів за методом Фаулера-Нордхейма через діелектрик, що не вимагає високої напруги і дозволяє зробити комірки мінімального розміру. Саме процес тунелювання заряду фізично зношує

комірки пам’яті. Зі збільшенням ємності мікросхеми флеш-пам’яті зменшується і загальна кількість циклів запису, оскільки комірки пам’яті стають все більш мініатюрними і для розсіювання оксидних перегородок, що ізолюють плаваючий заслін, потрібна все менша напруга. Зі збільшенням ємності проблема надійності тільки загострюється. Крім того, в перспективі флеш-пам’ять зіткнеться з новими проблемами: розміри чіпів продовжують зменшуватись, з електричних кіл відбувається витік струмів, і вони втрачають здатність зберігати дані після відключення живлення.

Одним з методів побудови енергонезалежних ЗП і усунення зазначених недоліків є використання властивостей окремих аморфних напівпровідників (халькогенідів) здійснювати фазовий перехід з непровідного аморфного стану (лог.1) в провідний кристалічний стан (лог.0).

Проведені теоретичні і експериментальні дослідження фірмами-розробниками доводять, що такі ЗП мають високу стійкість до дії іонізуючих опромінень, що робить їх перспективними для застосування в космічній галузі. У відомих працях запропоновані функціональні схеми ЗП на аморфних напівпровідниках, в яких вузли керування процесом запису і читання виконані на базі біполярних структур і до складу комірки пам’яті входять діоди або транзистори, виготовлені за біполярною технологією.

В цій праці пропонується комірку пам’яті виконати на базі аморфного напівпровідника і транзистора, емітер якого також виготовлений з аморфного напівпровідника. Це забезпечує підвищення радіаційної стійкості комірки пам’яті і, крім того, в перспективі це може дати можливість будувати ЗП для трійкової логіки, що буде сприяти підвищенню ефективності обробки інформації.

УДК 681.325+681.335

ПІДВИЩЕННЯ ТОЧНОСТІ ТА ШВИДКОДІЇ АЦП ІЗ ПЕРЕРОЗПОДІЛОМ ЗАРЯДУ ЗА РАХУНОК ВИКОРИСТАННЯ ВАГОВОЇ НАДЛИШКОВОСТІ

С. М. Захарченко, к.т.н., доцент
Винницкий национальный технический университет
zaxar@vstu.vinnica.ua

АЦП із перерозподілом заряду займають важливе місце серед сучасних перетворювачів послідовного наближення. Даний факт пояснюється специфічними ознаками таких пристроїв, зокрема: відносно проста структура, яка не потребує застосування пристрою вибірки-зберігання; мала споживана потужність, оскільки вихідний код формується в процесі перерозподілу заряду між конденсаторами матриці, висока швидкодія тощо.

Застосування вагової надлишковості дозволяє, з одного боку, зменшити вимоги до виготовлення базових аналогових компонентів, зокрема вимоги узгодження номіналів конденсаторної матриці, а з іншого боку підвищити точність і швидкодію за рахунок використання методів цифрового самокалібрування.

Стрибкоподібний характер змінення напруги на виході конденсаторної матриці дає додатковий резерв підвищення швидкодії. Так при застосуванні двійкової системи числення для забезпечення максимальної швидкодії необхідно забезпечити ідеальне узгодження сталої часу в усіх гілках матриці, при застосуванні вагової надлишковості такої необхідності немає.

Один із можливих варіантів реалізації АЦП із перерозподілом заряду із застосуванням вагової надлишковості наведено на рисунку.

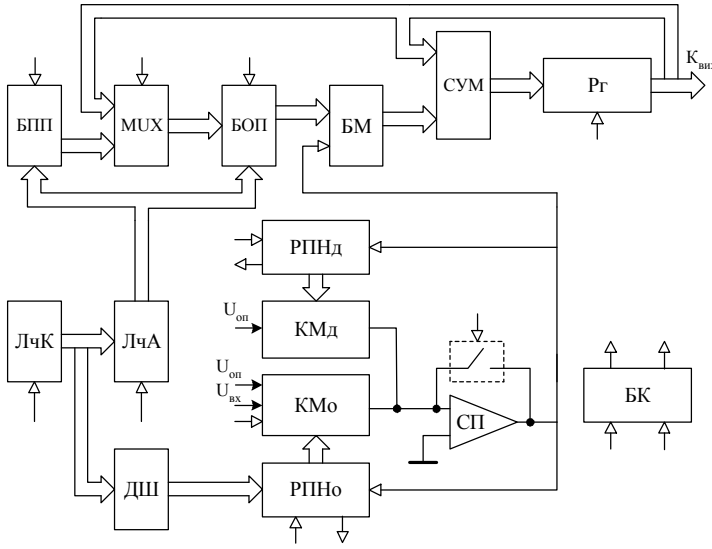


Рис. АЦП із перерозподілом заряду із застосуванням вагової надлишковості.

Пристрій працює в двох режимах: основному, коли він виконує свою основну функцію і режимі калібрування, в якому здійснюється визначення ваг «неточних» розрядів.

Аналогова частина містить основну і допоміжну конденсаторні матриці (КМо та КМд) та схему порівняння (СП). КМд використовується тільки в режимі калібрування для зменшення інструментальної похибки. Керування матрицями здійснюється відповідними регістрами послідовного наближення (РПН). Блок постійної пам’яті (БПП) містить значення ваг «точних» розрядів, що були виміряні на етапі виготовлення, блок оперативної пам’яті (БОП) містить як ваги «точних», так і «неточних» розрядів, які було визначено на етапі калібрування. Блок маскування (БМ), суматор (СУМ) та вихідний регістр (Рг) використовуються для формування вихідного коду шляхом додавання значень ваг розрядів, що знаходяться в оперативній пам’яті.

УДК 681.3:621.375

ВИРІВНЮВАННЯ КОЕФІЦІЄНТІВ ПЕРЕДАЧІ ПРОМІЖНИХ КАСКАДІВ ДВОТАКТНИХ ПІДСИЛЮВАЧІВ ПОСТІЙНОГО СТРУМУ

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

azarov@vstu.vinnica.ua

Деякі провідні компанії у галузі мікроелектроніки, такі як Analog Device, ON Semiconductor, Intersil та ін., випускають двотактні підсилювачі постійного струму (ППС). Перевагами таких пристроїв є висока лінійність передатної характеристики, гарні показники швидкодії, а також симетричність перехідної характеристики на вхідний двополярний імпульсний сигнал. Водночас, у серійних двотактних ППС існують проблеми завдання робочої точки їх проміжних каскадів. Вказана особливість заважає будувати схеми із високим загальним коефіцієнтом передачі.

Слід відзначити, що відомі двотактні симетричні ППС, побудовані як на польових, так і на біполярних транзисторах, мають загальний недолік – низький коефіцієнт підсилення. Традиційно ця проблема вирішується шляхом додаткового уведення проміжних відбивачів струму і нарощування кількості вихідних каскадів. Проте такий підхід призводить до зменшення ефективного підсилення на каскад і збільшення споживаної потужності мікросхем. Це значно обмежує номенклатуру, а також статичні характеристики мікросхем двотактних ППС, що випускаються серійно. Термін «симетричний»

означає рівність коефіцієнтів передачі верхнього і нижнього трактів підсилення, не зважаючи на те, що вони побудовані на транзисторах різного типу провідності, які мають різні коефіцієнти β підсилення по струму. Водночас використання двотактних структур потенційно може бути перспективним за умови вирішення проблеми забезпечення робочих точок проміжних підсилювальних каскадів. Це дозволило б збільшити коефіцієнт підсилення, а також зберегти високу лінійність передатної характеристики і симетричність перехідної характеристики.

Вирішувати вказану проблему автори пропонують за допомогою двох методів:

а) переведення вхідного двотактного каскаду у режим мікрострумів із подачою на вхід різницевого струму зміщення рис. 1;

б) застосування компенсаційних струмів, що формуються за допомогою двоконтурних зворотних зв'язків на основі двонаправленого відбивача струму (ДВС).

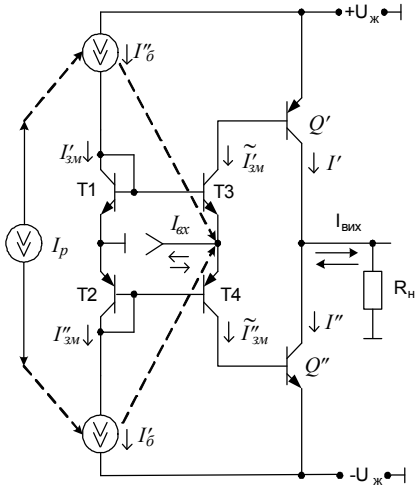


Рисунок 1 – Фрагмент схеми, що реалізує перший метод

Вказані методи вирівнювання коефіцієнтів передачі проміжних каскадів дозволяють також автоматично підтримувати номінальні режим роботи ППС, що в свою чергу дозволяє отримати високі динамічні та статичні характеристики схеми.

УДК 631.514

ЗАВАДОСТІЙКА СИСТЕМА КЕРУВАННЯ ПОТОКАМИ ДАНИХ НА ФОТОННИХ КРИСТАЛАХ

В. П. Кожем'яко, д.т.н., професор
О. А. Іванов, студент
Вінницький національний технічний університет
ali-arab@mail.ru

Область дослідження фотонних кристалів - одна із найбільш гарячих у світових наукових центрах, гігантах високотехнологічного бізнесу і на підприємствах військово-промислового комплексу.

На даний момент досягнення у вищеназваній області дають можливості для реалізації надзвичайно важливих задач оптоелектроніки, таких як зменшення втрат при мікро-згинах у оптичних хвилеводах, дають можливість для відсікання та суттєвого зменшення фотонного шуму. В залежності від методик виготовлення кристалів досягаються від'ємні коефіцієнти заломлення, це дає можливість фокусування випромінювання в область мешу за довжину хвилі. Але особливий інтерес становлять фотонні структури для керування потоками даних.

У наступній роботі буде виконано розрахунок та аналіз системи керування на фотонних кристалах. Завдяки поетапному розгалуженню в різних площинах отримаємо відносну простоту конструкції та можливість просторового керування лазерними пучком. Така структура дозволить направляти світло в одному з п'яти напрямків, що буде обиратись в залежності від потреб. При цьому абсолютно не важливо розташування самого лазера. Ця система знайде застосування у інтегральній оптичній техніці та системах для створення голограм.

При необхідності застосування пасивного керування, тобто рівномірного поділу потужності по напрямкам, доцільно застосовувати природній опал. Його властивості найкраще підходять для вирішення поставленої задачі.

При обробці опалу за методом двофотонної полімеризації можливо отримати лабіринти будь-якої складності у кристалі опалу. Включно і просторові канали. При поширенні світла у даній структурі практично відсутні втрати та зберігаються його основні характеристики.

Така реалізація знайде своє застосування у оптичній інтегральній схемотехніці, системах передачі даних, також становить інтерес для захисту інформації на апаратному рівні, оскільки малі розміри не дозволять таємного проникнення у систему.

УДК 681.325

ДИНАМІЧНА МОДЕЛЬ АНАЛОГО-ЦИФРОВОГО ПЕРЕТВОРЮВАЧА

В. М. Кичак, д.т.н., професор; С. Г.Бортник, аспірант;
Н. О. Пунченко, аспірант
Вінницький національний технічний університет
v_kychak@ukr.net

Аналого-цифрові перетворювачі (АЦП) відносяться до класу пертворювачів форми інформації, що широко застосовуються у сучасних засобах передавання та оброблення сигналів. Характеристики АЦП безпосередньо впливають на ефективність функціонування систем передавання та оброблення інформації. Динамічні властивості АЦП відображають їх здатність виконувати перетворення змінних у часі вхідних сигналів і можуть представлятись за допомогою повних динамічних характеристик. У загальному випадку АЦП є нелінійними пристроями, внаслідок чого побудова адекватних їм динамічних моделей і визначення повних динамічних характеристик є достатньо складною та до цього часу нерозв'язаною задачею.

У роботі пропонується динамічна модель АЦП, що враховує нелінійність характеристики перетворення (ХП) за допомогою введення у модель шумових компонентів. Такий підхід дозволяє застосовувати при нормуванні ХП клас лінійних операторів, враховуючи нелінійні властивості АЦП. В якості вхідного тестового впливу АЦП використовується синусоїдальний сигнал. За допомогою періодограмного методу оцінюються енергетичні спектри вхідного $X(f_i)$ та вихідного $Y(f_i)$ сигналів АЦП. На основі виразу для лінійної інерційної системи

$Y(f_i) = |K(f_i)|^2 \cdot X(f_i)$ знаходиться частотна характеристика АЦП $K(f_i)$. Визначена таким способом характеристика дозволяє виділити складові вихідного сигналу АЦП, що обумовлені лінійними інерційними ефектами досліджуваного перетворювача.

Згідно запропонованої методики на вихідний сигнал модельованого АЦП накладається ідеальний шум квантування. Модель АЦП будується на базі динамічної моделі Вінера, що містить послідовно з'єднані лінійний інерційний та нелінійний статичний блоки. Для врахування нелінійних ефектів аналого-цифрового перетворення в модель АЦП уведено адитивний рівномірно розподілений в інтервалі $[-q/2, q/2]$ шум квантування, де q - крок квантування.

Відповідно до традиційної спектральної методики для вихідного сигналу АЦП за результатами експериментальних досліджень визначається відношення сигнал/шум S/N_e. Такі ж оцінки даного відношення сигнал/шум були отримані розрахунковим шляхом для запропонованої динамічної моделі АЦП - S/N_m.

Аналіз результатів досліджень показав, що у смузі нижніх частот найбільш суттєвими є нелінійні властивості АЦП, а інерційні проявляються незначним чином. Відповідно теоретично отримані значення S/N_m у низькочастотній смузі переважають експериментальні оцінки S/N_e. У високочастотній смузі робочих частот спостерігається висока збіжність результатів моделювання та експериментальних досліджень.

Запропонована модель АЦП дає змогу підвищити точність аналізу функціонування перетворювачів аналог-код у динамічному режимі.

УДК 621.397

МЕТОД ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ ПАРАЛЕЛЬНО-ПОСЛІДОВНОГО АНАЛОГО-ЦИФРОВОГО ПЕРЕТВОРЮВАЧА

Г. Г. Бортник, к.т.н., доцент;
О. В. Стальченко, асистент; В. А. Челоян, аспірант
Вінницький національний технічний університет
bortnykg@mail.ru

Сучасні технології виготовлення не забезпечують високої завадостійкості аналого-цифрових перетворювачів (АЦП). Тому, коли технологічні можливості покращення шумових властивостей АЦП вичерпані, потрібні застосовувати принципово інші підходи, що базуються, зокрема, на введенні надлишковості на різних рівнях проектування перетворювачів. Актуальним напрямком для створення високоточних АЦП слід вважати розробку нових методів підвищення завадостійкості АЦП.

Для покращення шумових властивостей АЦП в структурах паралельно-послідовного аналого-цифрового перетворення (ППАЦП), разом з перекриттям шкал ступенів цих перетворювачів можна використовувати передбачення вхідного сигналу на момент його кодування АЦП молодшого рівня.

Визначення параметрів моделі передбачення з урахуванням фільтрувальних властивостей ППАЦП проведемо в часовій z-області. При розв'язанні цієї задачі, обрано критерій оптимального передбачення, що представляється таким виразом

$$E_{опт} = \min_{\alpha_k, \beta_l} M\left\{ \left[S_x(t_i) - S_{перед}(t_i, \alpha_k, \beta_l) \right]^2 \right\},$$

де $S_{перед}(t_i, \alpha_k, \beta_l)$ - вихідний сигнал передбачення, який залежить від часу та від вагових коефіцієнтів передбачення; $S_x(t_i)$ - сигнал, значення якого необхідно передбачити.

Для ППАЦП цей вираз прийме вигляд:

$$E_{опт}(b'_{k_{опт}}) = \min_{(b'_k)} M_i \left\{ \left[S_{вх}(t_i) - S_{перед}(t_i) \right]^2 \right\},$$

де $S_{вх}(t_i) = k_{АЦП} U_{вх}(t_i)$ - відлік вхідного сигналу АЦП.

Для визначення оптимального, відповідно до вибраного критерію, вектора коефіцієнтів передбачення $B' = \{b'_k\}$, $k = \overline{1,n}$, отримано таку систему:

$$R_{вз}(kT_д) = \sum_{l=1}^{n} b'_l \cdot R(|l-k| \cdot T_д),$$

де $R_{вз}(kT_д) = M_i \left\{ S_{вх}(t_i) \cdot S_{вих}(t_i - kT_д) \right\}$ - взаємна кореляційна функція вхідного та вихідного сигналів.

Виразимо взаємну кореляційну функцію $R_{вз}(kT_д)$ через автокореляційну функцію вихідного сигналу АЦП. При $S_{вх}(t_i) = S_{вх}(t_i) - \sum_{k=1}^{n} b'_k S_{вих}(t_i - kT_д)$ маємо $R_{вз}(kT_д) = R(kT_д) - \sum_{l=1}^{n} b_l \cdot R(|l-k| \cdot T_д)$, і система рівнянь прийме вигляд $V \times B' = C$, де $C = \{c_k\}$; $k = \overline{1,n}$; $c_k = R(kT_д) - \sum_{l=1}^{n} b_l \cdot R(|l-k| \cdot T_д)$; $V = \{V_{kl}\}$; $k = \overline{1,n}$; $l = \overline{1,n}$.

Одержана система рівнянь дозволяє визначити коефіцієнти передбачення b'_k, на базі яких можна реалізувати ППАЦП з підвищеною завадостійкістю.

УДК 621.382(07) + 681.32(07)

МЕТОД БАГАТОКАНАЛЬНОГО АНАЛОГО-ЦИФРОВОГО ПЕРЕТВОРЕННЯ МОНТЕ-КАРЛО

М. В. Лаврів, асистент
Прикарпатський національний університет
ім. В. Стефаника (м. Івано-Франківськ)
dlya_marii@mail.ru

Функціональним призначенням інфосистем є збір параметричної інформації перебігу інфопроцесів, перетворення, обробка та передача даних. Тенденції розвитку інфосистем полягають у застосуванні ефективних методів перетворення динамічних інфопараметрів (наприклад, швидкість, прискорення і т.п.). Пристрої аналого-цифрового перетворення, що входять до складу інфосистем, визначають техніко-економічні характеристики системи, тому критерій вибору методу аналого-цифрового перетворення повинен задовольняти поставлені техніко-економічні вимоги, забезпечувати достатню роздільну здатність, лінійність, точність, високий рівень завадозахисту при невисоких коштах виробництва.

Основні характеристики багатоканальних пристроїв діагностичних систем: кількість каналів, розрядність аналого-цифрового перетворювачів і швидкість передачі даних. В багатоканальних і багатопроцесорних інформаційно-вимірювальних системах застосовують часовий та просторовий розподіл каналів для зв’язку розподілених в просторі об’єктів вимірювання з центральним процесором. При часовому розподілу каналів використовують загальний АЦП з вхідним аналоговим комутатором каналів і послідовною розгорткою каналів у

часі. При просторовому розподілі каналів кожен з них містить свій АЦП, або застосовується багатоканальний АЦП з паралельною розгорткою значень загальної міри в каналах. Утворення багатоканальної системи з просторовим розділенням каналів, коли в кожному з каналів використовується окремий АЦП, вимагає великої кількості апаратури, в тому числі і пам'яті. Користувачі точних дельта-сігма перетворювачів вимушені застосовувати АЦП індивідуально на кожний із каналів внаслідок значного часу встановлення вхідних фільтрів, коли інтегруючі, багатокаскадні та АЦП послідовного перетворення дозволяють здійснювати багатоканальне мультиплексування.

Для використання в задачах вимірювання динамічних характеристик віброакустичних сигналів на перший план виносяться вимоги до характеристик точності та швидкодії. Забезпечення обох вказаних параметрів спричиняє до значних апаратурних затрат на реалізацію, що прямим чином відображається на вартості аналого-цифрових перетворювачів.

Поставлене завдання вирішується використанням АЦП Монте-Карло, який при простоті технічної реалізації забезпечує високу швидкість та точність перетворення, дозволяє значно розширити спектральну смугу перетворення, яке визначається якістю статистичного розподілу та спектральними характеристиками псевдовипадкового опорного сигналу перетворення. В практиці до цього часу широке застосування методу Монте-Карло обмежувалось алгоритмічною складністю та високими коштами побудови якісних генераторів псевдовипадкових сигналів.

УДК 621.382(07) + 681.32(07)

ДОСЛІДЖЕННЯ ХАРАКТЕРИСТИК ПОСЛІДОВНОСТЕЙ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ДЛЯ АЦП МОНТЕ-КАРЛО

М. В. Лаврів, асистент
Прикарпатського національного університету
ім. В. Стефаника (м. Івано-Франківськ)
dlya_marii@mail.ru

Аналогові елементи в засобах перетворення форми інформації вносять досить значні апаратурні спотворення, що зумовлює зниження точності та достовірності результату перетворення. Застосування методу аналого-цифрового перетворення Монте-Карло дозволяє реалізувати перетворювачі по складності та вартості порівнянні із послідовними АЦП, із можливістю адаптації частотних характеристиками, вищою точністю перетворення та інтегруванням відліків вхідного сигналу у функції часу. Якість перетворення таких засобів визначається якістю статистичних характеристик застосованого методу генерування псевдовипадкового опорного сигналу.

Найбільш загальними і істотними недоліками, що ускладнюють застосування генераторів випадкових чисел, є обмежена швидкодія; низька стабільність імовірнісних параметрів; складність апаратурної реалізації; неможливість відтворення і передбачення генерованих послідовностей в силу їх випадкового характеру. Це зумовило застосування в практиці методів генерування псевдовипадкових послідовностей на основі математичних методів синтезу таких числових послідовностей.

Аналіз методів та засобів генерування псевдовипадкових послідовностей дозволив визначити незадовільні техніко-економічні характеристики їх застосування в практиці, що зумовило необхідність розробки нових методів генерування з рівномірним характером розподілу на основі циклічних зсувів, реалізованих на регістрі зсуву, охопленому логічним зворотним зв'язком та сумуванням за *mod 2* (метод Ґалуа), а також із дзеркальним взаємним відображенням вагових номерів розрядів двійкових кодів на основі взаємної перестановки старших та молодших ваг вихідних розрядів двійкового лічильника.

Проаналізовано отримані результати досліджень статистичних характеристик та спектрального аналізу формованих послідовностей псевдовипадкових чисел, які дозволили зробити висновок про рівномірний характер розподілу псевдовипадкових числових послідовностей та ефективність застосування запропонованих методів для вирішення прикладних задач статистичних досліджень Монте-Карло

Порівняння результатів досліджень характеристик запропонованих методів генерування та відомих методів дозволяє зробити висновок про те, що найвищу достовірності обчислення площ фігур методом Монте-Карло можна досягнути внаслідок використання генератора із дзеркальним взаємним відображенням двійкових розрядів. При цьому слід вказати незначну величину похибки обчислень навіть при малих періодах генерованих послідовностей чисел.

Використання запропонованих методів генерування псевдовипадкових сигналів із рівномірним розподілом дозволило реалізувати високоточні методі та засоби інтегруючого аналого-цифрового перетворення Монте-Карло, структурні схеми яких наведено в доповіді.

УДК 681.3:621.375

СИСТЕМИ ЧИСЛЕННЯ З ВАГОВОЮ НАДЛИШКОВІСТЮ ДЛЯ ШВИДКОДІЮЧИХ АЦП ПОСЛІДОВНОГО НАБЛИЖЕННЯ І ЦАП, ЩО САМОКАЛІБРУЮТЬСЯ

О. Д. Азаров, д.т.н., професор; О. О. Решетнік, аспірант; М. Ю. Шабатура, студент
Вінницький національний технічний університет
de_gratnik@i.ua

Переважна більшість сучасних перетворювачів форми інформації (ПФІ) у вигляді АЦП і ЦАП реалізується з використанням класичної двійкової системи числення. Водночас у ряді випадків побудова АЦП і ЦАП на базі систем числення із ваговою надлишковістю дозволяє комплексно вирішувати проблеми підвищення швидкодії і точності АЦП, а також ЦАП побудованих на низькоточній елементній базі.

Принциповим недоліком використання двійкової системи числення у ПФІ є те, що наявність інструментальних статичних похибок призводить до появи в характеристиці перетворення ЦАП зон, в яких вихідну аналогову величину не можна набрати жодною кодовою комбінацією. Це у свою чергу, призводить до виникнення в АЦП, побудованому на такому ЦАП, так званих пропусків кодів. Для реалізації АЦП без пропусків коду треба використовувати ЦАП із ваговою надлишковістю, який не має розривів характеристики перетворення. Такий підхід, до того ж, спрощує калібрування ваг розрядів і дозволяє формувати результат перетворення в АЦП одночасно з компенсацією динамічних похибок. Слід відзначити, що наведений підхід дозволяє підвищувати точність багаторозрядних АЦП і ЦАП, побудованих на неточних

елементах (похибки 5% - 10%), шляхом самокалібрування ваг розрядів. Крім того є можливість значного (на один, два порядки) підвищення швидкодії АЦП порозрядного врівноваження.

Системою числення, або нумерацією, є сукупність прийомів та правил для найменування та позначення чисел. Набір ваг розрядів системи числення – це базис. Алфавіт – це множина значень які може приймати кожен розряд системи числення. Таким чином система числення може задаватись через основу системи числення, базис та алфавіт.

У системах числення з ваговою надлишковістю (СЧВН) із природним базисом виникають проблеми із точним зображенням цілих чисел. Водночас неточність представлення цілих чисел аж ніяк не впливає на точність перетворення аналог-код або код-аналог. Це є принциповим аргументом на користь СЧВН, оскільки в АЦП або ЦАП незалежно від того, яка в них використовується система числення завжди є інструментальні похибки на рівні половини молодшого розряду.

Слід зазначити, що побудова ПФІ на основі СЧВН вимагає створення специфічної елементної бази для кожної окремої СЧВН. Для подолання цього техніко-економічного бар`єру при практичній реалізації ПФІ автори пропонують кілька підходів щодо побудови ЦАП із ваговою надлишковістю на основі класичної ненадлишкової двійкової системи числення.

Таким чином використання СЧВН на основі двійкових рядів дає можливість будувати надлишкові ЦАП на базі двійкових ненадлишкових ЦАП, які не мають розривів передатної характеристики навіть при наявності відхилень ваг розрядів.

УДК 681.118.5

АЛЬТЕРНАТИВНІ МЕТОДИ ВІДОБРАЖЕННЯ ЦИФРОВИХ ДАНИХ У ТАЙМЕРНИХ ПРИСТРОЯХ

А. М. Пєтух, д.т.н., професор;
В. В. Войтко, к.т.н., доцент; Б. С. Гут, студент
Вінницький національний технічний університет
goot1986@mail.ru

Розвиток сучасних людино-машинних систем у період глобальної комп'ютеризації потребує використання динамічних засобів відображення інформації, підвищуючи вимоги до якісних характеристик сприйняття даних. У зв'язку з цим актуальними є питання реалізації принципів ергономіки у засобах візуалізації, що сприяє оптимізації процесів подання і сприйняття інформативних потоків.

Метою роботи є підвищення якісних характеристик процесів сприйняття даних у засобах відображення за рахунок впровадження альтернативних форм подання цифрової інформації, реалізованих з використанням принципів аналого-цифрового формування зображень.

Об'єктом дослідження постають процеси подання і сприйняття цифрової інформації та методи формування нових форм інформативного відображення. Предметом дослідження вважаємо цифрове зображення даних на етапі формування інформаційної моделі засобу відображення.

Основними задачами роботи вбачаємо розробку та дослідження альтернативних методів подання аналого-цифрової інформації у таймерних пристроях.

За допомогою одного обертового диску–табло можна реалізувати альтернативний годинниковий пристрій, який не потребує двох обертових стрілок (годинної та хвилинної) та базується на аналого–цифровому принципі подання даних. У модернізованому табло пропонуємо

використовувати дві шкали для відображення інформації про години і хвилини. Маска має вигляд обмеженого сектору з центральною індикаторною стрілкою. Робочий отвір маски розраховано для відображення двох годинних секторів з огляду на те, що одногодинний сектор буде сприйматись людиною як дещо обмежений часовими рамками конкретної ситуації, а три годинні сектори будуть харектеризуватись інформативною надлишковістю. Вигляд диску-табло і маски альтернативного годинникового пристрою показані на рис. 1,а.

Другу альтернативну модель пропонуємо як поєднання сумісних шкал, які синхронно заповнюються протягом плину часу (рис. 1,б). Внутрішня шкала відтворює секундний відлік і може слугувати користувачеві як окремий пристрій (секундомір), а дві зовнішні шкали поєднують формування хвилинно-годинного відтворення інформативних потоків, коли заповнення хвилинної градації спричиняє синхронне зафарбовування наступного відліку годинної шкали. Розмежування трьох шкал дозволяє без додаткового збільшення площі індикатора підвищити роздільну здатність сприйняття інформації у порівнянні зі звичайним аналоговим диском-табло, коли три стрілки рухаються в одному полі даних. Крім того, запропонований метод відображення часового простору виграє в інформативному плані порівняно зі стрілково-дисковим методом, за рахунок посилення відчуття пройденого часу і часу, котрий залишилось пройти в системі відліку кожної шкали.

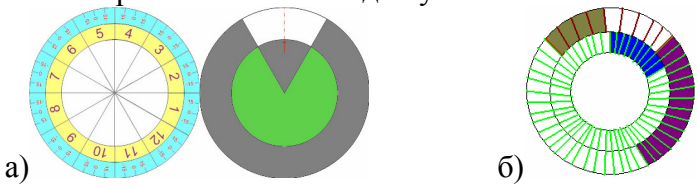


Рисунок 1 – Альтернативні моделі таймерних пристроїв

УДК 681.333

ПЕРЕТВОРЕННЯ ДАНИХ ПРИ МОДЕЛЮВАННІ НЕЙРОНА

Т. Б. Мартинюк, к.т.н., доцент
Н. В. Фофанова, аспірант
А. В. Ромигайло, студент; Л. В. Сидорук, студент
Вінницький національний технічний університет
lapka-carapka@mail.ru

Незважаючи на свою структурну і функціональну простоту, формальний нейрон (ФН) з пороговою функцією активації широко застосовується у нейромережах або у вхідному шарі для обмеження вхідних сигналів за певним порогом, або у вихідному шарі у нейромережах без зворотного зв'язку у цьому шарі. Особливо активно модель такого формального нейрона застосовується у біомедичних дослідженнях.

Основною проблемою при апаратній реалізації будь – якої моделі ФН є побудова просторово – часового суматора, оскільки необхідно реалізувати паралельне підсумовування зважених елементів вхідного векторного масиву даних. Одним з варіантів такого підсумовування можна розглядати оброблення даних за різницевими зрізами. Суть цього підходу полягає в тому, що порогове оброблення масиву чисел зводиться до обчислення і підсумовування часткових сум, порівняння цих сум з порогом і формування поточного порогу і відповідних вихідних даних (реакцій). Особливістю такого порогового оброблення масиву чисел є природний паралелізм, оскільки задіяні у формуванні часткових сум всі операнди, і нефіксоване (нестале) значення часу оброблення, яке залежить від кількості елементів на вході, кількості

однакових елементів, тобто від їх розподілу у масиві і від величини порогу. Це збільшує адекватність (наближення) реакції штучного нейрона до реакції біологічного нейрона через принцип формування його відгуку.

Отже, у запропонованій моделі ФН застосовано цифровий варіант відомого аналогового способу підсумування тривалостей групи часових інтервалів проф. Кожем'яко В.П., який є складовою запропонованого ним око – процесорного оброблення інформації для аналізу і розпізнавання сигналів і зображень.

УДК 621.317

ЗАСТОСУВАННЯ ЦИФРОВИХ ФІЛЬТРІВ ДЛЯ РЕАЛІЗАЦІЇ МЕТОДА СИМЕТРИЧНИХ СКЛАДОВИХ ФОРТЕСКЬЮ

Р. В. Петросян, старший викладач
Житомирський державний технологічний університет
e_rvs@ukr.net

Потреба в електричній енергії є однієї з найважливіших потреб сучасного суспільства. Електроенергія є особливим видом товару і має ряд специфічних властивостей. Як будь-яка продукція, електроенергія характеризується якістю. Проблема підвищення якості електричної енергії нерозривно з`вязана з проблемою ефективного енергозбереження.

Для виміру таких показників якості, як усталене відхилення напруги, коефіцієнти несиметрії напруг по зворотній послідовності та по нульовій послідовності застосовуют метод симетричних складових Фортескью. Чтоб його реализувати потрібно викорастати ДПФ. Однак це потребує великих обчислювальних витрат. Тому для усунення вказанного недоліка був розроблен метод, який базуеться на цифровій фільтрації.

Суть методу полягає у тому, що дані вводяться в пам'ять мікропроцесорного пристрою. Отриманий вхідний сигнал обробляється за допомогою 6 цифрових фільтрів. Цифрові фільтри реалізовані таким чином, щоб замінити складні вирази, використовувані в непрямих методах вимірювання показників якості електричної енергії. Крім того данний метод дозволив компенсувати частотну залежність методу, застосувавші цифрові фільтри з потрібною фазовою характеристикою.

УДК 681.3

КОДЕР/ДЕКОДЕР МОВНИХ СИГНАЛІВ НА БАЗІ ВИСОКОЛІНІЙНОГО АЦП ІЗ ВАГОВОЮ НАДЛИШКОВІСТЮ

О. Д. Азаров, д.т.н, проф.; С. В. Богомолов, магістрант
Вінницький національний технічний університет

Кодери/декодери для скремблювання мовних сигналів являють собою одну з галузей масової технічної діяльності, в якій за допомогою електроніки здійснюється обробляння, накопичення, кодування, декодування і розповсюдження в електричній формі сигналів звукового діапазону частот.

Сучасні кодери/декодери для скремблювання мовних сигналів розвиваються у двох основних напрямках. По-перше, поширене використання інтегральних схем і, по-друге, використання аналого-цифрової техніки не тільки для перетворення, а й для обробляння сигналів. У теперішній час способи перетворення та опрацювання мовних сигналів потребують аналого-цифрових пристроїв з досить високими характеристиками: динамічним діапазоном до 100-110 дБ і коефіцієнтом нелінійних спотворень близько 0,001÷0,002% .

Досягнення в розвитку цифрових технологій дозволили значно поліпшити якість опрацювання мовних сигналів. Одним із шляхів цього напрямку є побудова і використання високолінійних, швидкодіючих АЦП і ЦАП із ваговою надлишковістю. Найефективнішим шляхом створення перетворювачів форми інформації з високою лінійністю є застосування методів самокалібрування на основі надлишково-позиційних систем числення (НПСЧ) з використанням чисел Фібоначчі й «золотої пропорції». Застосування ж даних НПСЧ дозволяє також здійснювати

закриття та стиснення інформації методами, які ґрунтуються на властивостях даних систем.

Системний підхід до проектування АЦП і ЦАП, що самокалібруються, кодерів/декодерів для скремблювання мовних сигналів, включає аналіз необхідних характеристик перетворювачів інформації й синтез відповідних структурних і схемних рішень. При використанні АЦП і ЦАП виникає необхідність розгляду їх як сукупності аналогових і цифрових пристроїв (підсилювачів, комутаторів, пристроїв вибирання-зберігання, буферів і т.д.). Такий підхід дозволяє визначити статичні й динамічні складові загальної похибки й оптимізувати характеристики всього тракту проходження звукового сигналу.

У системах зв'язку відомо два основних методи скремблювання аналогових сигналів, що розрізняються по способу передачі по каналах зв'язку: аналогове скремблювання й дискретизація мови з наступним шифруванням.

Кожний із цих методів має свої переваги й недоліки.

Розглядаються принципи побудови аналогових і цифрових скремблерів, описано підхід до побудови скремблера на базі АЦП і ЦАП із ваговою надлишковістю, а також системи кодування із використанням НПСЧ. Використання даних систем числення забезпечує, по-перше, підвищення точності і швидкодії, по-друге, з точки зору короткочасного шифрування, робота в єдиному коді. Скремблери всіх типів вносять спотворення у відновлений мовних сигнал, тому проектування скремблерів аналогових сигналів на базі АЦП і ЦАП із ваговою надлишковістю із застосуванням властивостей надлишкових систем числення є актуальною для подальшого розвитку наукового напрямку у галузі створення кодерів/декодерів для скремблювання мовних сигналів.

УДК 681.325; 681.335

МІЖКАЛІБРУВАЛЬНИЙ ІНТЕРВАЛ ДЛЯ АЦП ПОРОЗРЯДНОГО КОДУВАННЯ ІЗ ВАГОВОЮ НАДЛИШКОВІСТЮ, ЩО САМОКАЛІБРУЮТЬСЯ

О. Д. Азаров[1], д.т.н., професор; О. В. Кадук[2], аспірант
Вінницький національний технічний університет
[1]azarov@vstu.vinnica.ua, [2]k67alex@yahoo.com

Застосування багаторозрядних АЦП послідовного наближення в інформаційно-вимірювальних системах, багатоканальних системах збору даних, системах управління та інше вимагає дотримання їх метрологічних характеристик протягом всього циклу експлуатації, а також при роботі у складних умовах. Слід відзначити, що за таких вимог у вказаних пристроях виникають параметричні відмови. Вони проявляються у зміні параметрів аналогових вузлів АЦП і призводять до виходу похибки перетворення за межі допуску. Це асоціюється з відмовою пристрою в цілому. Вказана проблема вирішується як шляхом удосконалення елементної бази, так і використанням різного роду коригувань і калібрувань. Для зменшення похибки перетворення перспективним є періодичне використання процедур самокоригування і самокалібрування в багаторозрядних ЦАП і АЦП із ваговою надлишковістю.

Поява похибок у вагах розрядів має наслідком появу похибок інтегральної і диференційної нелінійності на характеристиці перетворення АЦП порозрядного кодування із ваговою надлишковістю. Ймовірність того, що дійсне значення ваги розряду Q_i буде знаходитися у межах технологічного допуску δQ, маючи нормальний закон розподілу значень ваг розрядів, можна визначити як:

$$p = \frac{1}{\sigma\sqrt{2\pi}} \int_{\overline{Q_i}-\Delta Q_i}^{\overline{Q_i}+\Delta Q_i} e^{-\frac{\left[Q_i-\left(\overline{Q_i}+\Delta\overline{Q}_i\right)\right]^2}{2\sigma^2}} dQ,$$

де $\Delta\overline{Q}_{i\,T} + \Delta\overline{Q}_{i\,t} = \Delta\overline{Q_i}$ - загальні змінення ваги розряду під впливом температури і в часі. Відносне значення математичного сподівання похибки, що обумовлена параметричними відмовами, буде визначатися як:

$$M(\delta Q_{INL}) = \frac{\alpha^n - 1}{\alpha^{n+p} - \alpha^p} q,$$

де α - основа системи числення, q - ймовірність відмови i-го розряду, p - параметр надлишкового коду.

Слід зазначити, що під час змінення температури ΔT або функціонування ПФІ протягом часу Δt може з'явитись параметрична відмова з ймовірністю p (рис. 1).

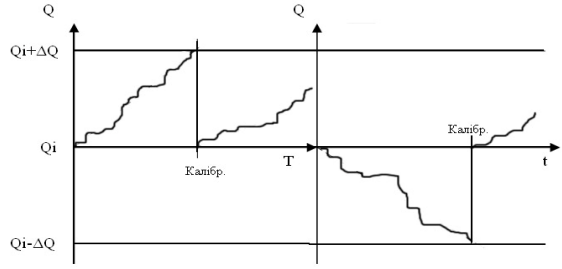


Рис. 1. Поява похибки АЦП при зміні температури і в процесі старіння

При цьому збільшується ймовірність появи похибки перетворення АЦП, значення якої виходить за межі допуску. Відповідно для її усунення необхідно виконувати самокалібрування ваг розрядів перетворювача форми інформації з інтервалом $\Delta T = \pm\delta Q / \mu_{Q_i}$, де μ_{Q_i} – температурний коефіцієнт, або при зміненні температури навколишнього середовища на $\Delta t = \pm\delta Q / \nu_{Q_i}$, де ν_{Q_i} – коефіцієнт часової нестабільності.

УДК 681.3

МЕТОДИ ПІДВИЩЕННЯ ТОЧНОСТІ КАЛІБРУВАННЯ АЦП ПОСЛІДОВНОГО НАБЛИЖЕННЯ ПРИ ЗАСТОСУВАННІ ВАГОВОЇ НАДЛИШКОВОСТІ

С. М. Захарченко, к.т.н, доцент; М. Г. Захарченко, старший викладач; О. В. Бойко, студент
Вінницький національний технічний університет
zahar@vstu.vinnica.ua

Аналого-цифрові перетворювачі є основною ланкою, що пов'язує світ природних аналогових сигналів з цифровими системами керування, діагностування, збору та обробки аналогової інформації, тощо. Саме тому точність, швидкодія та інші характеристики цих пристроїв безпосередньо впливають на параметри систем до складу яких вони входять. Вищезгадані вимоги обумовили популярність такого різновиду перетворювачів, як АЦП із перерозподілом заряду, належать до перетворювачів послідовного наближення і, відповідно характеризуються досить високою роздільною здатністю на рівні 14-16 двійкових розрядів та середньою швидкодією. Традиційним методом забезпечення високої роздільної здатності є застосування методів калібрування старших розрядів перетворювача. Однак при використанні двійкової системи числення процедура калібрування може виконуватись виключно в цифроаналоговій формі, що, по-перше, вимагає застосування додаткових коригувальних матриць, а по-друге, виконується в режимі реального часу. Інший підхід передбачає будувати АЦП із використанням вагової надлишковості. В даному випадку процедура калібрування може виконуватись виключно в цифровій

формі. Однак відомі методи реалізації таких пристроїв вимагають застосування так званих додаткових розрядів, тобто поширення розрядної сітки в бік молодших розрядів, або передбачають досить складні процедури розрахунку, що суттєво ускладнює обчислювальну частину пристрою.

Метою роботи є розробка методу самокалібрування АЦП із перерозподілом заряду, який, з одного боку забезпечить зменшення методичної похибки самокалібрування без застосування додаткових розрядів, а з іншого боку не вимагатиме складних математичних обрахунків.

Вихідним положенням для самокалібрування є розбиття розрядної сітки перетворювача на групи так званих «точних» та «неточних» розрядів. Кордон між вказаними групами визначається роздільною здатністю перетворювача та технологічною похибкою виготовлення конденсаторної матриці. Процес цифрового самокалібрування передбачає застосування вагової надлишковості, тобто

$$\frac{Q_i}{Q_{i-1}} < 2$$

В даному випадку будь-який розряд перетворювача може бути представлений сумою кількох молодших розрядів. Для зменшення методичної похибки калібрування пропонується проводити згадану процедуру для кожного розряду кілька разів, примусово забороняючи включення того чи іншого молодшого розряду. Отримані в результаті цих калібрувань значення мають бути осереднені.

Базовим припущенням методу є наявність незначних відхилень ваг точних розрядів за умови що сумарна похибка цих розрядів не перебільшує ваги молодшого розряду.

Наукове видання

МЕТОДИ ТА ЗАСОБИ КОДУВАННЯ, ЗАХИСТУ Й УЩІЛЬНЕННЯ ІНФОРМАЦІЇ

Тези доповідей
другої Міжнародної науково-практичної конференції
м. Вінниця 22-24 квітня 2009 року

Матеріали подаються в авторській редакції

Видавництво ВНТУ «УНІВЕРСУМ-Вінниця»
Свідоцтво Держкомінформу України
серія ДК №746 від 25.12.2001
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ,
гол. корпус, к. 114 тел. (0432) 59-85-32

Підписано до друку 27.04.2009 р.
Гарнітура Times New Roman.
Формат 29,7×42¼ Папір офсетний.
Друк різографічний. Ум. друк. арк. 11,78
Наклад 70 прим.. Зам. № 2009-086

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