УДК 004.383

В.С. Глухов, Р. Еліас
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

УБУДОВАНИЙ КОНТРОЛЬ СПЕЦПРОЦЕСОРІВ ДЛЯ ОБРОБЛЕННЯ ЦИФРОВИХ ПІДПИСІВ

Оцінено ефективність убудованого контролю помилок при множенні елементів поля GF(2^m) у гауссівському нормальному базисі типу 2 для спецпроцесорів оброблення цифрових підписів, що ґрунтуються на еліптичних кривих. Гауссівський нормальний базис типу 2 рекомендований Державним стандартом України ДСТУ 4145-2002. Для таких базисів парність арифметичного (у полі GF(2^m)) добутку двох елементів поля дорівнює парності їхнього логічного добутку, що покладено в основу методу. Також описано засоби проектування спецпроцесорів, які дають змогу оцінювати ефективність вбудованих вузлів виявлення помилок.

Ключові слова: поле Галуа GF(2^m), гауссівський нормальний базис типу 2, множення, контроль на парність, вбудований контроль.

In the article efficiency of concurrent error detection for elements of the Galois field GF(2^m) multiplication in Gaussian normal basis of type 2 which used in elliptic curves digital signature algorithm is estimated. Gaussian normal basis of type 2 is used according to State standard of Ukraine DSTU 4145-2002. For such basis parity of arithmetic (in the GF(2^m)) multiplication of two field elements is equal to parity of their logical product, that is laid in basis of method. Also in the article the development environment for dedicated processors which allow concurrent error detection efficiency estimating is described.

Keywords: Galois field GF(2^m), Gaussian normal base of type 2, multiplying, parity check, concurrent error detection.

Вступ

Сучасні стандарти для роботи з цифровими підписами основані на використанні полів Галуа *GF*(2^m) та еліптичних кривих. Формування та перевірка цифрових підписів складається з послідовності операцій над точками еліптичних кривих, кожна з таких операцій, своєю чергою, складається з послідовності операцій додавання та множення елементів полів Галуа *GF*(2^m).

Елементи $\{q, q^2, q^{2^2}, ..., q^{2^{m-1}}\}$ основного поля Галуа GF(2^m) утворюють нормальний базис (θ – корені полінома *p*, що утворює поле). Усі інші елементи основного поля Галуа GF(2^m) можуть бути подані у нормальному базисі (у вигляді $a_0 q + a_1 q^2 + a_2 q^{2^2} + ... + a_{m-1} q^{2^{m-1}}$), де a_i – двійкові розряди (i = = 0, 1, …, *m-1*).

Розрядність елементів поля *m* може сягати 2048 бітів. Апаратна реалізація помножувача для таких полів вимагає більш ніж мільйона транзисторів, що призводить до зростання ймовірності помилок у його роботі. У публікаціях останніх років звертається увага на вбудовані (*CED - concurrent error detection*) методи виявлення помилок у роботі помножувачів за допомогою цифрового контролю на парність (порівняння кількості 1 серед бітів операндів та результатів).

Державний стандарт України рекомендує використовувати для обробки цифрових підписів, що ґрунтуються на еліптичних кривих, гауссівський нормальний базис типу 2. Для такого базису парність арифметичного (у полі *GF*(2^m)) добутку двох елементів поля дорівнює парності їхнього логічного

добутку. Простота реалізації методу компенсується його невисокою надійністю, метод дає змогу виявляти лише 50 % помилок множення. У статті оцінюється надійність цього методу під час оброблення цифрових підписів. Показано, що ймовірність виявлення помилок під час оброблення цифрових підписів з використанням цього методу наближається до 100 %.

Також у статті розглянуто технологічні засоби для проектування і дослідження спеціалізованих процесорів, які містять вузли вбудованого контролю. Одним з таких спеціалізованих процесорів є пристрій для формування та перевіряння цифрових підписів.

Постановка проблеми

Одним з методів контролю правильності виконання множення елементів поля Галуа $GF(2^m)$ є контроль на парність. Контроль вимагає додаткових апаратних або часових витрат і виявляє лише 50 % помилок множення. Тому актуальною є задача визначення доцільності використання цього методу під час оброблення цифрових підписів. Також актуальною є загальна задача розроблення технологічних та нагоджувальних засобів для проектування пристроїв з вузлами вбудованого контролю і доведення доцільності використання останніх.

Аналіз основних досліджень та публікацій

Гауссівський нормальний базис типу 2 рекомендує для використання Державний стандарт України [1]. У роботах [2, 3] наведено вдосконалений метод та схему вбудованого контролю множення елементів поля $GF(2^m)$ у цьому базисі, для якого ознака помилки множення $E_R = \sum_{i=0}^{m-1}(a_i b_i \oplus r_i)$, де a_i, b_i – біти елементів поля A та B; r_i – біти результату R.

Цілі статті

Метою статті є обґрунтування доцільності використання у спеціалізованих процесорах для оброблення цифрових підписів помножувача елементів поля $GF(2^m)$ з вбудованим контролем, який виявляє усього 50 % помилок множення, а також розроблення комплексу програм для проектування спецпроцесорів з вузлами вбудованого контролю та доведення доцільності використання останніх.

Алгоритмічні та математичні основи

Під час контролю роботи функціонального вузла на парність ознака помилки результату $E_R = P_R^{'} \oplus P_R$, де P_R – біт парності результату; $P_R = \sum_{i=0}^{m-1} r_i$, r_i – біти результату R; P'_R – передбачувана парність результату.

У гауссівському нормальному базисі типу 2 поля $GF(2^m)$ $P_R^{'} = \sum_{i=0}^{m-1} a_i b_i$ тому $E_R = P_R^{'} \oplus P_R = \sum_{i=0}^{m-1} a_i b_i \oplus \sum_{j=0}^{m-1} r_j = \sum_{i=0}^{m-1}(a_i b_i \oplus r_i)$.

Підсумовування всюди відбувається за модулем 2.

За відсутності помилки E_R=0. Ймовірність виявлення помилки для цієї схеми дорівнює 50 %.

Під час множення двох елементів (A та B) поля Галуа $GF(2^m)$ у нормальному базисі (далі множення у нормальному базисі) старший розряд результату $r_{m-1} = A*M*B^t$, де M – характерна для вибраного поля помножувальна матриця. Наступні розряди результату $(r_{m-2}, \ldots, r_0)$ обчислюються за цією самою формулою, тільки замість векторів A та B використовуються їхні послідовні циклічні зсуви на один розряд ліворуч. У полі Галуа $GF(2^m)$ елементами матриці M будуть тільки 0 та 1, при використанні гауссівського нормального базису типу 2 кількість 1 у матриці буде мінімально можливою і дорівнюватиме $2m$-1. Схема вузла помножувача з вузлом виявлення помилок наведена на рис. 1 [2].

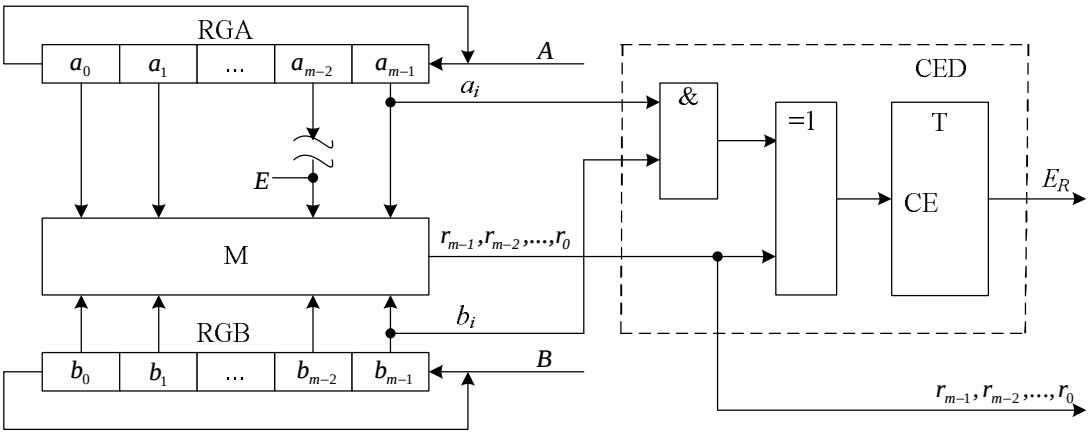

Рис. 1. Помножувач з CED (модель помилки № 1)

Дослідження вбудованого контролю множення у гауссівському нормальному базисі типу 2

Рис. 1 містить також модель помилок у роботі помножувача, які досліджувалися: обрив на одному з входів помножувальної матриці. Розглядалися дві ситуації: коли обірваний вхід сприймається як 0 (E=0) і коли обірваний вхід сприймається як 1 (E=1). Досліджувалася поведінка детектора помилок при формуванні цифрового підпису для тестового прикладу, наведеного у додатку Б.2 [1]. Результати тестування містять рис. 2 (для випадку E=0) та рис. 3 (для випадку E=1).

Для цього самого тестового прикладу досліджувалася реакція детектора помилок у разі внесення помилки до матриці M помножувача. Математична матриця M у розглянутому тестовому прикладі має розміри 173 рядка по 173 біти. Моделювалася поведінка детектора помилок при інверсії біта у 0-му рядку та у 172-му рядку матриці. Результати дослідження містять рис. 4, 5 відповідно.

Як видно з наведених графіків, кількість послідовних операцій множення під час оброблення одного цифрового підпису сягає 8983. З них більше ніж у 2000 детектор виявляє помилки.

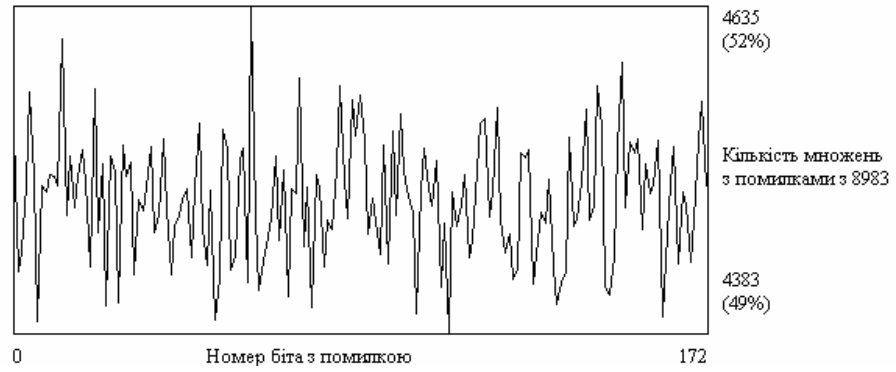

Рис. 2. Модель помилки № 1 (E = 0)

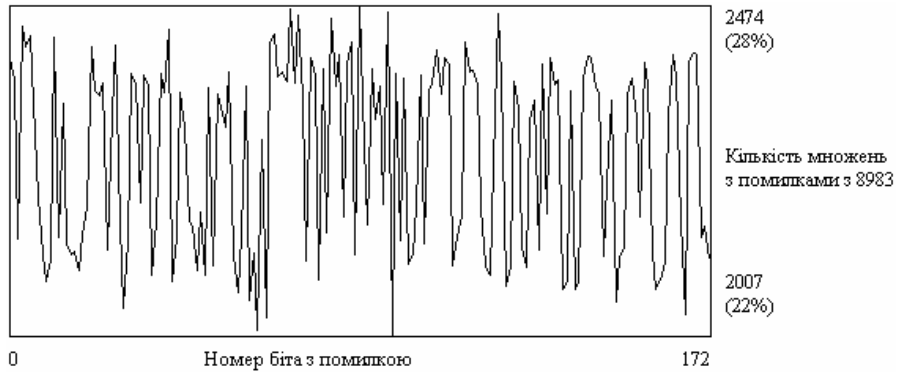

Рис. 3. Модель помилки № 1 (E = 1)

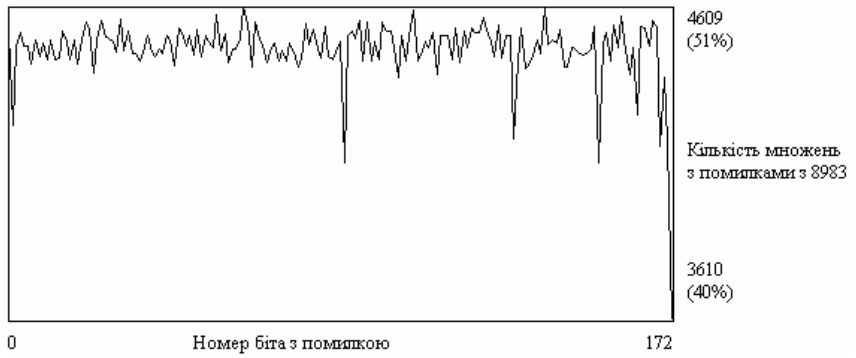

Рис. 4. Модель помилки № 2 (помилка в 0-му рядку матриці M)

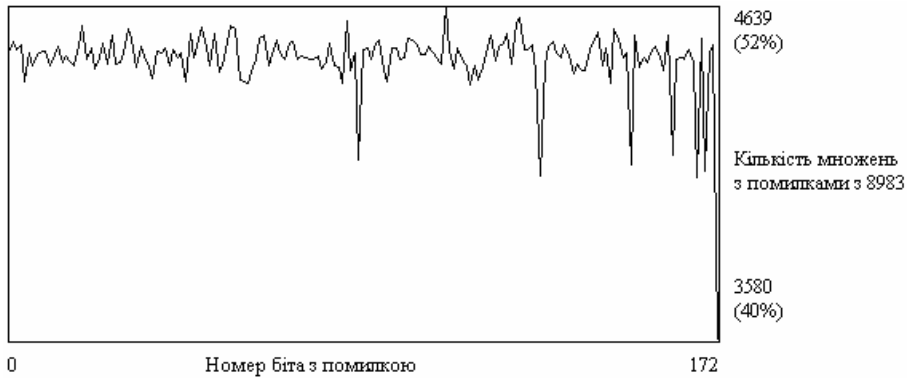

Рис. 5. Модель помилки № 3 (помилка в 172-му рядку матриці M)

Імовірність виявлення помилки помножувача під час оброблення цифрових підписів

Позначимо як p імовірність виявлення помилки у роботі помножувача. Імовірність невиявлення помилки $q = 1 - p$. Для k послідовних множень імовірність невиявлення помилки $Q = q^k = (1\text{-}p)^k$. Імовірність виявлення помилки у послідовності множень $P = 1 - Q = 1 - (1 - p)^k$.

Для $p = 0{,}5$, $k = 8983$ маємо $Q = 0{,}5^{8983} = 1/2^{8983}$ (імовірність підбору 173-бітного особистого ключа в наведеному прикладі становить $I = 1/2^{173}$, тобто набагато більша, ніж імовірність невиявлення помилки помножувача під час оброблення цифрових підписів).

Засоби проектування та дослідження вузла вбудованого контролю

Пристрій для формування і перевіряння цифрового підпису (обчислювач цифрового підпису згідно з [1]) входить до складу шифропроцесора, який забезпечує конфіденційність гарантоздатних систем (рис. 6). Шифропроцесор має дворівневу структуру. На верхньому рівні міститься протокольний універсальний процесор, який забезпечує зв'язок із зовнішнім світом і керує нижнім рівнем. На нижньому рівні розміщено декілька спецпроцесорів, одним із них є обчислювач цифрового підпису згідно з [1]. Протокольний процесор і спецпроцесори реалізовані на програмованій логічній інтегральній схемі (ПЛІС). Своєю чергою, спецпроцесор також має аналогічну дворівневу структуру (рис. 7). Протокольний RISC-процесор, який входить до складу спецпроцесора, може бути не обов'язково універсальним. Помножувач елементів поля Галуа $GF(2^m)$ входить до складу ядра спецпроцесора (рис. 7).

Послідовність проектування реалізованого на ПЛІС спецпроцесора з вузлом вбудованого контролю ілюструє рис. 8. Спецпроцесор призначений для формування і перевіряння цифрових підписів, але викладені нижче принципи можуть бути задіяні для проектування й інших спеціалізованих пристроїв.

Особливість цього підходу полягає в тому, що:

процес проектування спецпроцесора ділиться на чотири паралельні нитки:

програмування протокольного RISC-процесора;

проектування апаратного забезпечення ядра спецпроцесора (де розміщений помножувач з вузлом вбудованого контролю);

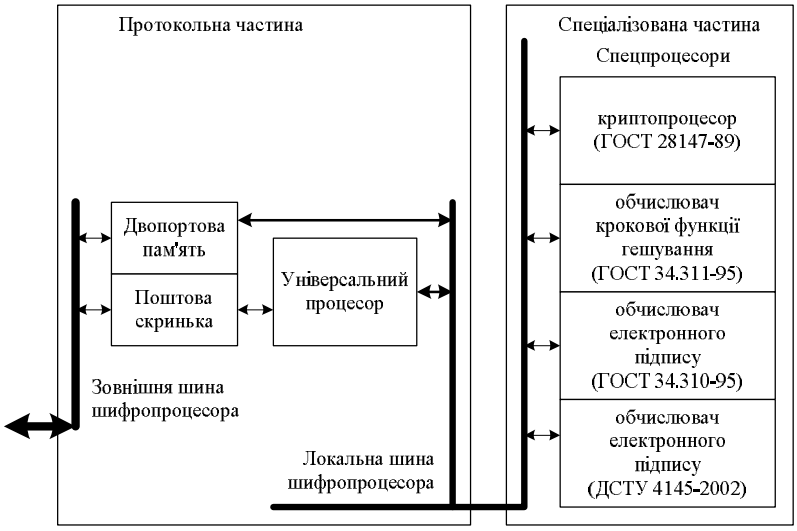

Рис. 6. Шифропроцесор

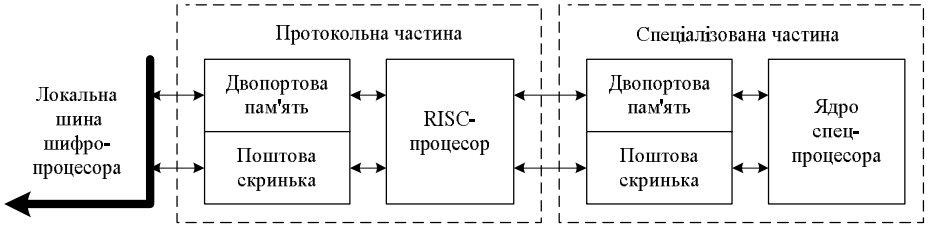

Рис. 7. Спецпроцесор

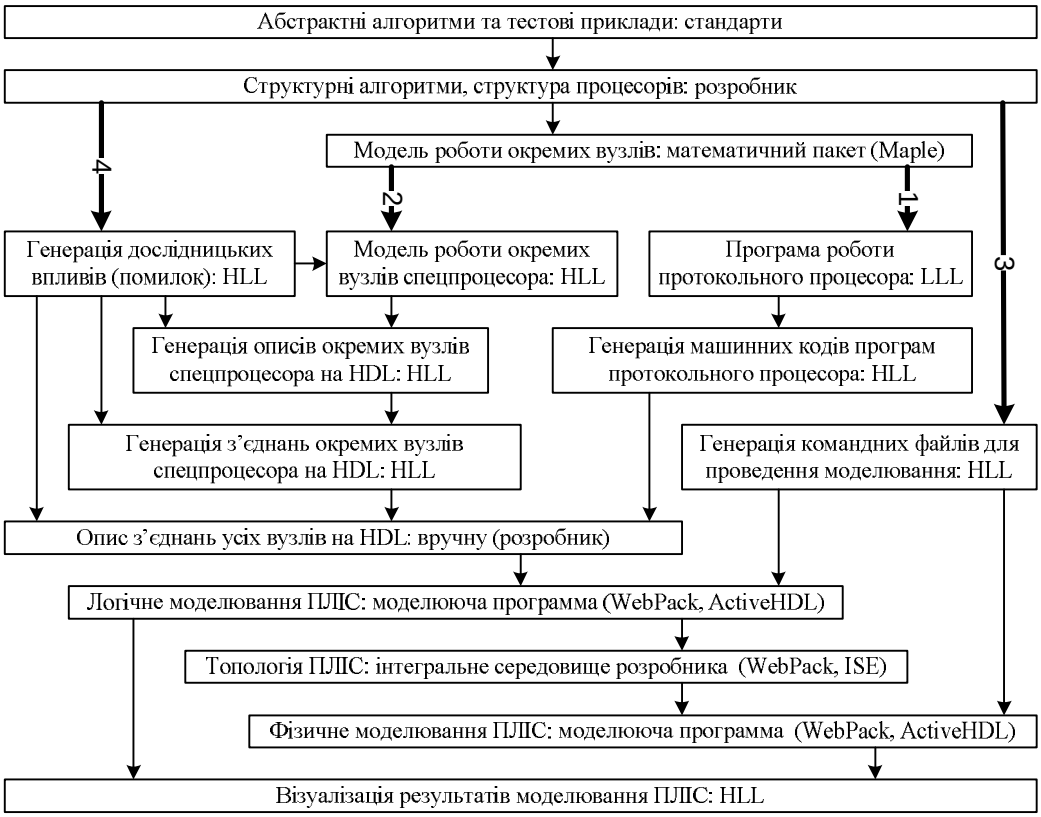

Рис. 8. Послідовність проектування описів функціональних вузлів

проектування командних файлів для засобів моделювання та перевірки роботи як універсального протокольного процесора, так і апаратного забезпечення спецпроцесора, проектування системи візуалізації та документування результатів досліджень;

проектування засобів дослідження поведінки спецпроцесора. Ці засоби забезпечують внесення помилок в описи окремих вузлів та спецпроцесора загалом для перевіряння роботи вузлів вбудованого контролю. Результати, наведені на рис. 2–5, отримано за допомогою цих засобів);

засоби програмування протокольного RISC-процесора забезпечують:

формування системи команд процесора;

написання програм роботи процесора мовою його асемблера;

синтаксичний контроль програм, написаних мовою асемблера протокольного RISC-процесора;

трансляцію програм з мови асемблера у машинні коди (LLL), формування завантажувальних файлів для ПЛІС;

проектування відбувається "зверху-донизу-вверх": від абстрактних алгоритмів до детальних описів окремих вузлів, а потім до перевіреної засобами моделювання топології кристала усього пристрою;

створення описів роботи вузлів мовоюі високого рівня (*HLL*-описів) відбувається одночасно з розробленням програм-трансляторів цих описів на мову опису апаратного забезпечення (*HDL*-описів). Такий підхід уможливлює моделювання функціональних вузлів, описаних мовою високого рівня. Якщо результати моделювання задовольняють розробника, відбувається трансляція описів з мови високого рівня (*HLL*-описів) на мову описів апаратних засобів (*HDL*-описів);

перевірка створених *HLL*-описів відбувається одночасно з перевіркою *HDL*-описів;

розроблювані *HLL*-описи та *HDL*-описи утворюють бібліотеку описів, елементи якої використовуються під час створення проекту загалом;

проектування може починатися з порожніми бібліотеками *HLL*- та *HDL*-описів;

з'єднання розроблених *HDL*-описів відбувається на етапі генерації *HDL*-опису вузла вищого рівня;

загальне з'єднання *HDL*-описів усіх вузлів в один проект відбувається в ручному режимі.

Для моделювання роботи апаратного забезпечення використовуються пакети *ActiveHDL (Aldec)*, *WebPack* або *ISE (Xilinx)*. Для проектування топології кристала ПЛІС застосовують засоби розробника ПЛІС - *WebPack* або *ISE* (*Xilinx*).

Засоби дослідження поведінки спецпроцесора генерують дослідницькі впливи – вносять помилки в наявні (раніше перевірені) *HDL*- або *HLL*-описи вузлів спецпроцесора і фіксують поведінку вузла вбудованого контролю.

Цей метод передбачає володіння розробником мовою програмування високого рівня (*HLL)*, низького рівня (*LLL)* та мовою описів апаратних засобів (*HDL)*.

Запропонований метод реалізований у вигляді комплексу програм. Метод розрахований на проектування спеціалізованих вузлів. Результати його застосування (бібліотеки описів, програми-генератори) є спеціалізованими і нині не можуть бути використані для розв'язання задач іншого класу.

Висновки

У статті обґрунтована доцільність використання у спецпроцесорах оброблення цифрових підписів помножувача елементів поля $GF(2^m)$ з вбудованим контролем, який виявляє усього 50 % помилок множення. Показано, що при цьому імовірність виявлення помилки оброблення цифрового підпису дуже близька до 100 %. Для поля $GF(2^{173})$ імовірність виявлення помилки дорівнює $1 - 1/2^{8983}$. Цей метод вбудованого тестування пропонується застосовувати під час роботи у нормальному базисі типу 2 полів $GF(2^n)$, які рекомендовані до використання стандартом ДСТУ 4145-2002. Також у статті описано комплекс програм, який забезпечує проектування та тестування спеціалізованих процесорів, зокрема тестування роботи вузлів вбудованого контролю.

1. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – К.: Державний комітет України з питань технічного регулювання та споживчої політики. 2003. 2. Глухов В.С. Вбудований контроль множення в гауссівському нормальному базисі типу 2 полів Галуа GF(2^m) // Науково-технічний журнал "Радіоелектронні і комп'ютерні системи" 6(47). Національний аерокосмічний

університет ім. М.Є. Жуковського "Харківський авіаційний інститут". – Харків: "ХАІ", 2010. – С. 255–259. 3. Глухов В.С., Еліас Р. Виявлення помилок при знаходженні оберненого елемента в гауссівському нормальному базисі типу 2 полів Галуа GF(2^m) // Науково-технічний журнал "Радіоелектронні і комп'ютерні системи" 6(47). Національний аерокосмічний університет ім. М.Є. Жуковського "Харківський авіаційний інститут". – Харків. "ХАІ", 2010. – С. 129–134.

УДК 681.142.2; 622.02.658.284; 621.325

Д.Д. Пелешко, Ю. Пелех, Н.О. Кустра, Т.В. Свірідова
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

РОЗРОБЛЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ ОБЛІКУ ПРОДУКЦІЇ

Розроблено програмне забезпечення для реалізації системи обліку продукції на виробництві. Розглянуто алгоритми обробки зображень, на яких ґрунтується робота системи. Описано інтерфейс програмного продукту та результати його роботи.

Ключові слова: автоматизація виробництва, бінаризація.

In this paper software for releasing of system for accounting of industrial goodsis developed. Algorythms of images processing is discussed. User interface of software is presented.

Keywords: production automation, binarization.

Вступ

Автоматизація повсюдно вважається головним, найперспективнішим напрямом розвитку промислового виробництва. Завдяки звільненню людини від безпосередньої участі у виробничих процесах, а також високій концентрації основних операцій значно поліпшуються умови праці та економічні показники виробництва.

Сьогодні системи автоматизованого керування є об'єктами активних досліджень. Дослідники, використовуючи новий технологічний рівень, повернулись до створення моделей комплексної автоматизації процесів виробництва. Для цього активно розробляється системно незалежне програмне забезпечення [1]. Основна проблема полягає у створенні системи протоколів функціювання мережі, оскільки автоматизовані системи керування ставлять нові вимоги до її функціювання: можливість роботи у режимі реального часу, максимальний пріоритет у роботі з об'єктом керування, надійність протоколів зв'язку з об'єктами і самотестування системи на предмет втрати зв'язку з контрольованим процесом.

Автоматизація промислових виробництв неоднакова. Вона дає найбільший ефект у виробництвах з масовим випуском продукції і порівняно працемісткими технологічними процесами.

Автоматизована система обліку на виробництві може створюватися за такими методиками:

- створення необхідної кількості автоматизованих робочих місць, призначених для вирішення певних облікових завдань;
- організація системної комп'ютеризації обліку, тобто об'єднання всіх автоматизованих робочих місць в єдину комп'ютерну мережу. В такому разі весь обсяг інформації в мережі стає доступним всім користувачам;
- створення все новіших і новіших комп'ютерних програм ведення обліку;