УДК 681.325.5-181.4

В. Глухов
Національний університет “Львівська політехніка”,
кафедра електронних обчислювальних машин

ОЦІНЮВАННЯ АПАРАТНИХ ВИТРАТ НА РЕАЛІЗАЦІЮ БАГАТОРІВНЕВОЇ КОМП’ЮТЕРНОЇ СИСТЕМИ З ВРАХУВАННЯМ ЗАКОНА АМДАЛЯ

Сформульовано підхід до оцінювання апаратних витрат на реалізацію багаторівневої комп’ютерної системи.

In this article multilevel computer system complexity estimation is discussed.

Вступ

У роботі пропонується метод оцінювання апаратних витрат на реалізацію багаторівневих комп’ютерних систем з врахуванням закону Амдаля для паралельних систем. Метод ґрунтується на використанні багаторівневої моделі взаємозв’язку відкритих систем. Також пропонується метод проектування багаторівневих систем, до якого метод оцінювання входить як складова частина.

Постановка проблеми

Велике значення при проектування засобів захисту інформації має їхня порівняльна оцінка, так само, як і оцінка складності алгоритмів, які реалізують ці засоби. Основою для реалізації засобів захисту інформації є багаторівневі системи. Водночас питання визначення складності багаторівневих ієрархічних систем ще не вирішено. Також не з’ясовано питання практичної реалізації теоретичних результатів на сучасному етапі розвитку, коли треба давати відповіді на запитання: «Чи можна певну багаторівневу систему реалізувати на ПЛІС із відомими характеристиками?» або «Які характеристики повинна мати ПЛІС для реалізації заданої багаторівневої системи?». Тому актуальним є питання оцінювання складності багаторівневих систем. Одному із методів рішення присвячена дана стаття. Пропонований метод ґрунтується на використанні закону Амдаля для паралельних систем.

Аналіз основних досліджень та публікацій

Однією з складових частин гарантоздантості [1, 5] є конфіденційність [6, 7]. Криптографічні методи забезпечення конфіденційності ґрунтуються на використанні шифропроцесорів (ШП). У роботі [8, 9] представлена багаторівнева структура ШП, який здійснює криптографічні перетворення відповідно до стандартів [10–13]. Для побудови ШП використовується центральний протокольний процесор і криптографічний спецпроцесор (або декілька спецпроцесорів), причому спецпроцесори можуть бути виконані у вигляді ядер НВІС [14]. Відомі декілька методів взаємодії центрального і спеціалізованого процесорів. Центральний процесор може сприймати спецпроцесор як співпроцесор, як набір портів і як канал [15, 16]. Протокольний процесор може одночасно керувати роботою декількох спецпроцесорів. Логічно така структура утворює зірку, а з’єднується протокольний процесор із спеціалізованими за допомогою локальної шини (магістралі). Так утворюється зірково-магістральна структура, переваги якої доведені у [17, 18].

Стандарти, чинні в України, повністю визначають алгоритми роботи усіх спецпроцесорів шифропроцесора. Міжнародні стандарти [19] є цінним і корисним доповненням до вітчизняних стандартів.

Протокольні процесори можуть бути реалізовані в складі ПЛІС [10, 20] або ззовні ПЛІС. Вони можуть бути RISC-процесорами та CISC-процесорами, 8-, 16-, 32-розрядними або можуть мати іншу розрядність [20]. Сучасні ПЛІС дають змогу реалізовувати універсальні процесори різного типу і продуктивності: *hard*-процесори (апаратно-реалізовані і розміщені на кристалі ПЛІС у процесі її

виробництва нереконфігуровані процесори) і *soft*-процесори [20] (реконфігуровані, розроблені користувачем ядра [14]).

Загалом основою для побудови багаторівневих комп'ютерних систем є багаторівнева модель взаємозв'язку відкритих систем [21, 22]. Найдоступнішим для проектування типом НВІС є програмовані логічні інтегральні схеми (ПЛІС), які відрізняються своїми технічними характеристиками (кількість і структура логічних боків, блоків введення-виведення, комутаторів і т. ін. [23]). Тому актуальним є завдання вибору ПЛІС для реалізації гарантоздатної конфіденційної системи у вигляді багаторівневої комп'ютерної системи. Велике значення при проектуванні засобів захисту інформації має їхнє порівняльне оцінювання, так саме, як і оцінювання складності алгоритмів, які реалізують ці засоби. Теорія алгоритмів і теорія складності розвинута у роботах [24–30]. Водночас питання визначення складності багаторівневих ієрархічних систем вирішене недостатньо. Спроба оцінити складність системи, до складу якої входять протокольний процесор і декілька спецпроцесорів, без врахування рівня паралелізму у роботі спецпроцесорів зроблена у [31]. Вплив рівня паралелізму на продуктивність системи визначають декілька законів, зокрема закон Амдаля [32].

Цілі статті

Метою роботи є створення на основі закону Амдаля для паралельних систем методу оцінювання апаратних витрат на реалізацію багаторівневих комп'ютерних систем, зокрема гарантоздатних. Метод повинен враховувати ієрархічність багаторівневих систем і ґрунтуватися на оцінці апаратних витрат на реалізацію кожного з рівнів. Також метою статті є розроблення методу проектування багаторівневих систем, до якого метод оцінювання повинен входити як складова частина.

Еталонна модель взаємозв'язку відкритих систем

Найбільш структуровано принцип побудови багаторівневих систем викладено у [21], де наведено базову семирівневу еталонну модель взаємозв'язку відкритих систем (рис. 1, 2). Основи обміну даними між сумісними рівнями ілюструє рис. 5, де фігурують протокольний та сервісний блоки даних (звідси випливає необхідність мати у складі *N*-рівня протокольний та спеціалізований процесор). Рис. 1 ілюструє універсальний характер моделі, оскільки не фіксує назви рівнів, а вказує їхні умовні номери (…, *N*+1, *N*, *N*-1, …).

Структура багаторівневої гарантоздатної системи

Згідно з [1] гарантоздатність визначає міру здатності об'єкта бути працездатним і виконувати покладені на нього функції у будь-який час виконання покладеної на нього місії за умови, що на початку виконання місії об'єкт був придатний до виконання цих функцій. Система гарантоздатна, коли вона доступна, надійна, безпечна, захищена (здатна зберігати конфіденційність, забезпечувати цілісність), ремонтопридатна. Кожний об'єкт гарантоздатної (з погляду конфіденційності) системи можна представити у вигляді дворівневої (бортова ЕОМ і ШП) системи [9]. ШП є засобом протистояння діям ворожого оточення, на нього покладаються завдання криптографічного захисту та верифікації інформації.

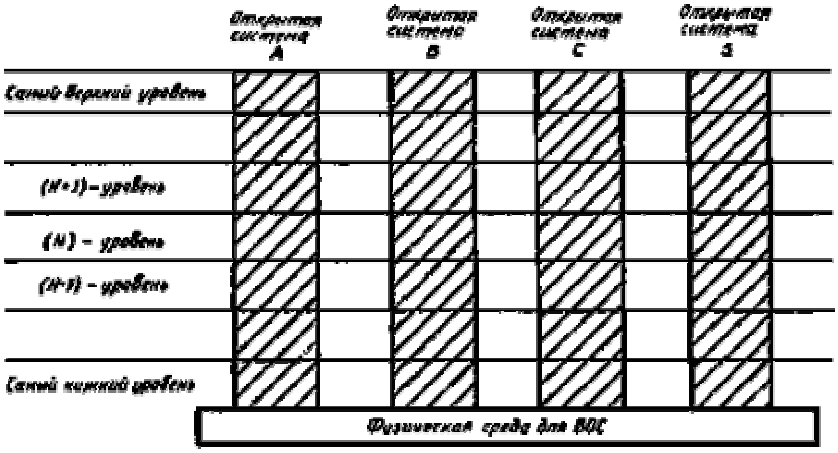

Рис. 1. Еталонна модель взаємозв'язку відкритих систем

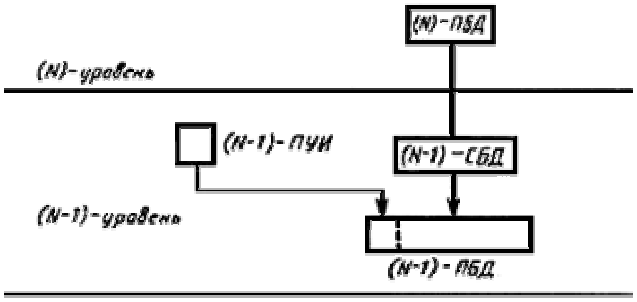

Рис. 2. Приклад перетворення блоків даних у суміжних рівнях

ПУИ – протокольна керуюча інформація, ПБД – протокольний блок даних, СБД – сервісний блок даних.

Для побудови ШП використовується центральний процесор і криптографічний спецпроцесор (або декілька спецпроцесорів), при цьому спецпроцесори можуть бути виконані у вигляді ядер НВІС [14].

Представлення спецпроцесора як каналу підказує використання еталонної моделі взаємозв'язку відкритих систем [21] для розподілення функцій між елементами системи. Взаємодія між бортовою ЕОМ і шифропроцесором відбувається на протокольному (найвищому) рівні. Потік інформації під час її оброблення в шифропроцесорі послідовно йде з найвижчого рівня на найнижчий, а потім знову підіймається на найвищий (наприклад, під час шифрування відкрита інформація опускається з верхнього рівня на найнижчій, а потім зашифрована інформація підіймається з найнижчого рівня на найвищий (рис. 3)).

Кожний *N*-рівень ШП є *N*-спецпроцесором, який складається з протокольного *N*-процесора і (*N*-1)-спецпроцесора. Усі спецпроцесори мають аналогічну структуру (рис. 4).

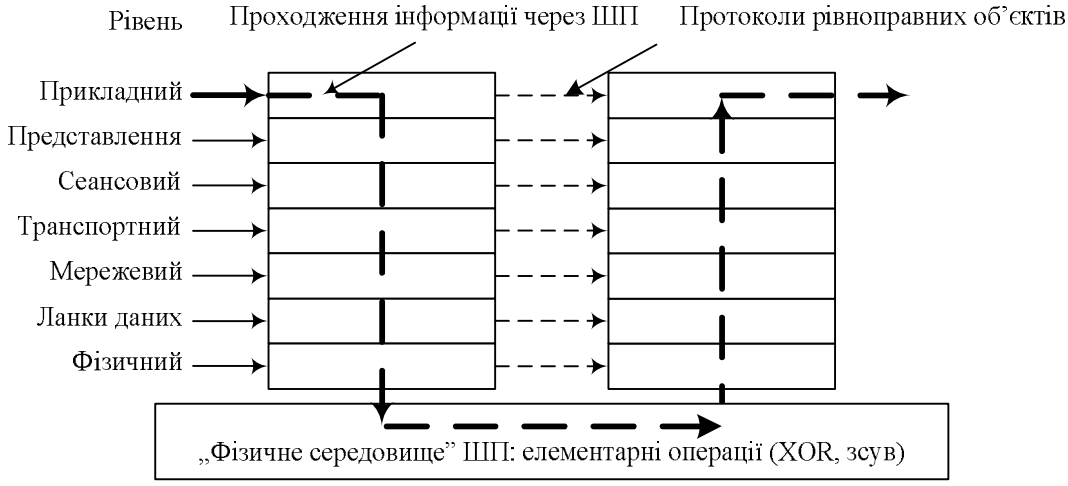

Рис. 3. Структура шифропроцесора

Апаратні витрати на реалізацію протокольного процесора і спецпроцесора

Найважливішим показником у теорії складності, яка оперує поняттям *SH*-модель, є апаратна складність [30]. На практиці це призводить до першочергового оцінювання апаратних витрат на реалізацію проектованої системи.

Визначення відношення кількості мікросхем або інших логічних елементів (вентилів, конфігурованих логічних блоків, в *SH*-моделі – елементарних перетворювачів [30]) у складі протокольного спеціалізованого процесора і дає змогу оцінити апаратні витрати на реалізацію першого, якщо відомі аналогічні витрати на реалізацію другого.

У парі «центральний процесор – математичний співпроцесор» відношення k кількостей транзисторів коливається у діапазоні k=0,6…3,0. У парі «центральний процесор – відеопроцесор» діапазон менший (k=0,7…1,3) і для процесорів з більшою кількістю транзисторів наближається до 1 [31]. Це значення може бути взяте за основу для оцінювання апаратних витрат на реалізацію

процесорів. Тобто, наближено можна прийняти, що апаратні витрати на реалізацію спецпроцесора дорівнюють апаратним витратам на реалізацію протокольного процесора (k=1).

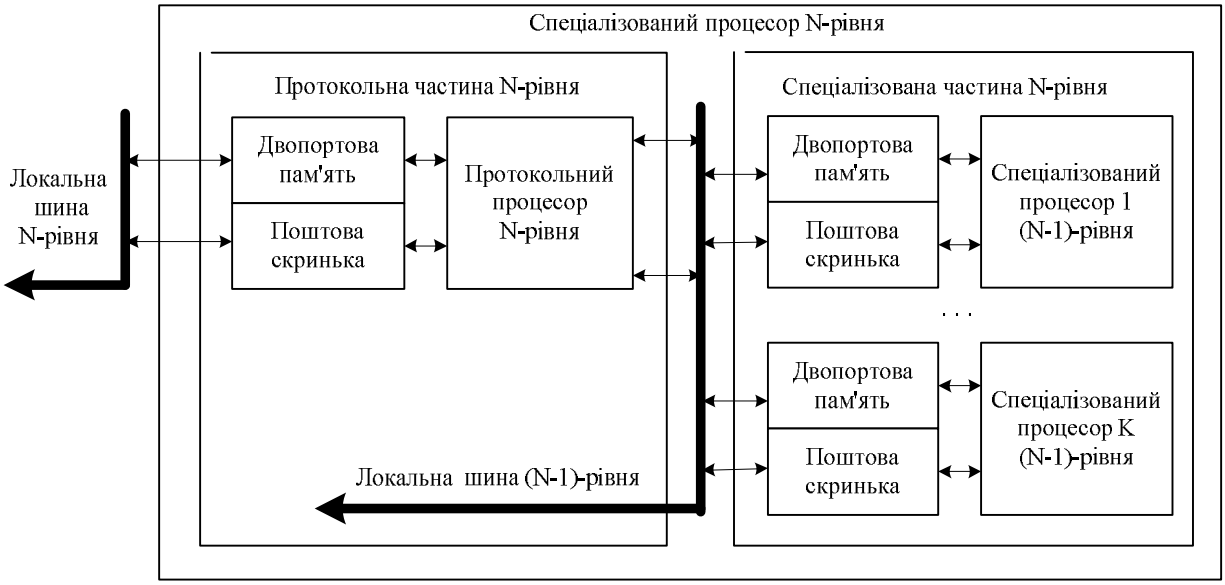

Рис. 4. Структура N-спецпроцесора (N-рівня)

Якщо вважати, що значення k є приблизно однаковим для усіх рівнів, то можна оцінити апаратні витрати на реалізацію усієї багаторівневої системи. Якщо позначити апаратні витрати на реалізацію спецпроцесора найнижчого (першого) рівня як v, то апаратні витрати на реалізацію кожного з рівнів при наведених припущеннях показано в табл. 1.

Таблиця 1

Апаратні витрати

Рівень	Апаратні витрати на реалізацю спецпроцесора	Апаратні витрати на реалізацію протокольного процесора	Апаратні витрати на реалізацію рівня
1	v	vk	v(1+k)
2	v(1+k)	v(1+k)k	$v(1+k)^2$
3	$v(1+k)^2$	$v(1+k)^2k$	$v(1+k)^3$
4	$v(1+k)^3$	$v(1+k)^3k$	$v(1+k)^4$
5	$v(1+k)^4$	$v(1+k)^4k$	$v(1+k)^5$
6	$v(1+k)^5$	$v(1+k)^5k$	$v(1+k)^6$
7	$v(1+k)^6$	$v(1+k)^6k$	$v(1+k)^7$

При кожному переході з верхнього рівня на нижчий апаратні витрати на реалізацію протокольного процесора доцільно зменшувати приблизно удвічі (в 1+k разів). Зменшення апаратних витрат призводить або до зменшення розрядності (32, 16, 8), або до зменшення набору функціональних вузлів, або до скорочення системи команд.

Апаратні витрати на протокольний процесор і декілька спеціалізованих процесорів

Протокольний процесор N-рівня може одночасно керувати роботою декількох (m) спецпроцесорів (N-1)-рівня. Логічно така структура утворює зірку, а з'єднання протокольного процесора із спеціалізованими здійснюється з допомогою локальної шини (магістралі). Тобто утворюється зірково-магістральна структура, переваги якої доведені у [17, 18].

Для спецпроцесорів, що працюють паралельно, доцільно уточнити апаратні витрати на реалізацію протокольного процесора за принципами закону Амдаля для паралельних систем.

Закон враховує частку S даних, які не обробляються паралельно (одночасно) усіма спецпроцесорами ($0 \le S \le 1$): чим вона менша, тим більший рівень паралелізму. Якщо $S=1$, спецпроцесори працюють послідовно у часі, якщо $S=0$ – паралельно у часі.

Для оцінки апаратних витрат комплект (N-1)-спецпроцесорів представляється одним еквівалентним спецпроцесором із продуктивністю P_{N-1}, яка дорівнює сумарній продуктивності усіх (N-1)-спецпроцесорів , визначеної за законом Амдаля для паралельних систем. Вважатимемо, що апаратні витрати на реалізацію цього умовного спецпроцесора зростають лінійно із зростанням продуктивності. Тоді апаратні витрати на реалізацію протокольного процесора будуть в k разів більші за витрати на реалізацію умовного спецпроцесора порівняно з витратами на реалізацію комплекту реальних спецпроцесорів.

За законом Амдаля зростання c продуктивності систем з m пристроїв, що працюють паралельно $c = \frac{1}{S + \frac{1-S}{m}} = \frac{m}{S(m-1)+1}$. Вважаємо, що так зростатимуть і апаратні витрати на реалізацію умовного спецпроцесора відносно одного спецпроцесора. Результати оцінювання апаратних витрат містять загалом апаратні витрати vn на реалізацію n-рівня системи з однаковими для усіх її рівнів *коефіцієнтами* k *та* m дорівнюватимуть $vn=van=v(m+ck)n=va1n$. для усієї *n-рівневої* системи апаратні витрати обчислюють як суму членів геометричної прогресії і дорівнюють $p=va1(a1n-1)/(a1-1)$, де $ai=(m+ck)i=a1i$ – коефіцієнт зростання апаратних витрат на реалізацію *i-го* рівня відносно 1-го рівня системи. У табл. 2 V – апаратні витрати на реалізацію одного спецпроцесора).

Загалом апаратні витати V_N на реалізацію N-рівня системи з однаковими для усіх її рівнів коефіцієнтами k та m дорівнюватимуть $V_N=vA_N=v(m+ck)^N=vA_1^N$. Для усієї N-рівневої системи апаратні витрати обчислюють як суму членів геометричної прогресії і дорівнюють $P=vA_1(A_1^N-1)/(A_1-1)$, де $A_i=(m+ck)^i=A_1^i$ – коефіцієнт зростання апаратних витрат на реалізацію i-го рівня відносно 1-го рівня системи.

Таблиця 2

Уточнені за законом Амдаля апаратні витрати для декількох спецпроцесорів

Варіант	Принцип роботи m спецпроцесорів	Апаратні витрати A_p на реалізацію m спецпроцесорів	Апаратні витрати A_y на реалізацію умовного спецпроцесора (A_y=Vc)	Апаратні витрати $A_п$ на реалізацію протокольного процесора ($A_п=A_y$k)	Апаратні витрати A на реалізацію рівня ($A=A_p+A_п$)
1	послідовно у часі (S=1, c=1)	Vm	V	Vk	V(m+k)
2	паралельно у часі (S=0, c=m)	Vm	Vm	Vmk	Vm(1+k)
3	загальний випадок (0<S<1, 1<c<m)	Vm	Vc	Vck	V(m+ck)

Метод проектування багаторівневих гарантоздатних комп'ютерних систем (у частині забезпечення конфіденційності)

Узагальнений метод проектування багаторівневих гарантоздатних комп'ютерних систем (у частині забезпечення конфіденційності) складається з послідовності проектних рішень:

система представляється як багаторівнева структура відповідно до еталонної моделі взаємозв'язку відкритих систем;

визначається кількість рівнів N;

кожний N-рівень шифропроцесора є N-спецпроцесором, який складається з протокольного N-процесора і деякої кількості (N-1)-спецпроцесорів;

визначається рівень паралелізму у роботі (N-1)-спецпроцесорів та їхня сумарна продуктивність A_{N-1}. Для оцінювання апаратних комплект (N-1)-спецпроцесорів представляється одним еквівалентним умовним спецпроцесором із продуктивністю A_{N-1};

кожний протокольний N-процесор реалізується як універсальний процесор;

продуктивність та інтерфейси універсального процесора визначаються особливістю системи;

кожний із спецпроцесорів реалізує одне із завдань (або декілька завдань, або частину завдань) забезпечення конфіденційності;

кожний із спецпроцесорів працює відповідно до обраного стандарту;

система команд спецпроцесора визначається алгоритмом вирішення відповідного завдання;

кількість спецпроцесорів визначається потоком даних та заданим часом їхнього опрацювання;

процесори реалізуються у вигляді ядер НВІС (практично – ПЛІС), утворюючи так звану «систему на кристалі»;

визначаються апаратні витрати v на реалізацію спецпроцесорів рівня 1 та усього рівня 1 (vA_1). За однаковою структурою кожного рівня апаратні витрати P на реалізацію усієї N-рівневої системи будуть орієнтовно дорівнювати $P=vA_1(A_1^N-1)/(A_1-1)$, що дає змогу обрати тип ПЛІС.

Висновки

У роботі запропонований і обґрунтований метод оцінювання апаратних витрат на реалізацію багаторівневих комп'ютерних систем, який ґрунтується на використанні багаторівневої моделі взаємозв'язку відкритих систем і законі Амдаля для паралельних систем. Також аналізуються апаратні витрати на реалізацію кожного рівня. За цим підходом можна оцінити можливість реалізації багаторівневої системи на ПЛІС конкретного типу на ранніх стадіях проектування, створити модульну ієрархічну структуру, до якої застосовуються методи паралельного і одночасного проектування, виготовлення, налагодження і тестування. Також пропонується метод проектування багаторівневих систем, до якого метод оцінювання входить як складова частина.

1. Military handbook MIL-HDBK-338b. Electronic reliability design handbook. Department of defense of USA. 1 october 1998. 2. Харченко В.С. Гарантоздатність комп'ютерних систем: проблеми і результати // Авіаційнокосмічна техніка і технологія. – 2005. – № 7 (23). – С. 352–376. 3. Харченко В.С. Гарантоспособность и гарантоспособные системы: элементы методологии / В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2006. – Вип 5(17). – С. 7 – 19. 4. Харченко В.С. Гарантоздатність комп'ютерних систем: проблеми, напрямки досліджень, результати // Радіоелектроннії комп'ютерні системи. – 2006. – № 5 (17). – С. 105–109. 5. Харченко В.С. Гарантоздатність комп'ютерних систем: межа універсальності в контексті інформаційно-технічоного стану / В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2007. – № 8. – С. 8–16. 6. IEC 50(191):1990 International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service. 135 p. 7. IEC 60050-191-am2 (2002) Ed. 1.0 International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service. 8. Глухов В., Заіченко Н., Оліярник Б. Шифропроцесор для бортових інформаційно-керуючих систем // Наукові нотатки: Міжвузівський збірник (за напрямком «Інженерна механіка»). Луцький державний технічний університет, Луцьк. 2007. – вип. 19 (січень 2007). – С.33–43. 9. Глухов В.С., Євтушенко К.С., Заіченко Н.В., Оліярник Б.О. Криптографічні засоби спеціалізованої бортової ЕОМ для бронетехніки // Вісник Хмельницького нац. ун-ту. 2007. – №2. Т. 2. – С. 29–33. 10. 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. 11. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Государственный комитет СССР по стандартам. – Москва, 1989. 12. Межгосударственный стандарт ГОСТ 34.311–95. Информационная технология. Криптографическая защита информации. Функция хеширования. Межгосударственный совет по стандартизации, метрологии и сертификации. – Минск: Госстандарт Украины, с дополнениями, 1997. 13. Межгосударственный стандарт ГОСТ 34.310–95. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. Межгосударственный совет по стандартизации, метрологии и сертификации. – Минск. Госстандарт Украины, с дополнениями, 1997. 14. Мельник А.О., Коркішко Т.А. Система підтримки виконання алгоритмів криптографічного захисту інформації на основі програмованого процесора та криптографічних акселераторів // Вісник Держ. ун-ту "Львівська політехніка"

«Комп'ютерні системи та мережі». 2000. – № 385. – С. 77 – 80. 15. Аронов В.Б., Глухов В.С., Деревенко Я.К., Заиченко Н.В., Федуняк С.Ф. Одноплатный арифметический процессор, подключаемый к магистрали ГОСТ 26765.51-86, и средства обеспечения его серийного производства // "I Научно-техническая конференция НПО "Фазотрон": Тезисы докладов. – Москва, 19-21 сентября 1989 г. 16. Глухов В.С., Заиченко Н.В. Арифметический спецвычислитель с кэш-памятью команд. "Тезисы докладов 29-й научно-технической конференции НПО "Антей". – Москва, 1990 г. 17. Николайчук Я.Н. Низовые вычислительные сети: Учеб. пособие. – К.: УМК БО, 1990. – 55 с. 18. Николайчук Я.М., Круцкевич Н.Д. Перспективи використання зірково-магістральної архітектури з пам'яттю колективного доступу в комп'ютерних мережах з глибоким розпаралелюванням // Вимірювальна та обчислювальна техніка в технологічних процесах: Збірник наукових праць – Хмельницький: ТУ/7. – 2002. – №9. – Т2. – С.122–126. 19. IEEE Std 1363-2000 IEEE Standard Specifications for Public-Key Cryptography Sponsor Microprocessor and Microcomputer Standards Committee of the IEEE Computer Society. Approved 30 January 2000. 20. Березко Л.О., Троценко В.В. Мультипроцесор на ПЛІС // Вісник Нац. ун-ту "Львівська політехніка". – 2006. – № 573. – С.10–14. 21. ДСТУ ISO/IEC 7498-1:2004. Інформаційні технології. Взаємозв'язок відкритих систем. Базова еталонна модель. Ч. 1. Базова модель (ISO/IEC 7498-1:1994, IDT). 22. ГОСТ 28906-91 (ИСО 7498-84, ИСО 7498-84 Доп.1-84). Системы обработки информации. Взаимосвязь открытых систем. Базовая эталонная модель. 23. Грушвицкий Р.И., Мураев А.Х., Угрюмов Е.П. Проектирование систем на микросхемах программируемой логики. – СПб.: БХВ-Петербург, 2002. – 608 с.: ил. 24. Черкаський М.В. Моделі неформальних алгоритмів // Вісник Нац. ун-ту "Львівська політехніка". – 2000. – № 385. – С.131 – 133. 25. Черкаський М.В. SH-модель алгоритму // Вісник Нац. ун-ту "Львівська політехніка". – 2001. – № 433. – С.127 – 134. 26. Мельник А.О. Черкаський М.В. Теорія алгоритмів і методи обчислень: новий курс // Вісник Нац. ун-ту "Львівська політехніка". – 2001. – № 437. – С.99 – 105. 27. Черкаський М.В., Мітюков В.С. Історичний аспект складності алгоритму // Вісник Нац. ун-ту "Львівська політехніка". 2002. – № 463. – С.111–118. 28. Черкаський М.В. Еволюція тлумачення поняття "алгоритм" // Вісник Нац. ун-ту "Львівська політехніка". – 2003. – № 492. – С.142 – 146. 29. Черкаський М.В., Саїд Садек Абдалла. Псевдо SH-модель // Вісник Нац. ун-ту "Львівська політехніка". – 2004. – № 523. – С.145 – 150. 30. Черкаський М.В., Хусейн Халід Мурад. Універсальна SH-модель // Вісник Нац. ун-ту "Львівська політехніка". – 2004. – № 523. – С.150 – 154 . 31. Глухов В.С. Оцінка апаратних витрат на реалізацію багаторівневої комп'ютерної системи // Вісник Нац. ун-ту «Львівська політехніка». – 2008. – № 629. – С.13–20. 32. Shekhar Borkar. Thousand Core Chips – A Technology Perspective. DAC 2007, June 4–8, 2007, San Diego, California, USA. Copyright 2007 ACM 978-1-59593-627-1/07/0006.