Національна академія наук України
Інститут кібернетики імені В. М. Глушкова

На правах рукопису

ГРИГОРУК Павло Михайлович

ПРИНЦИПИ ОБРОБКИ ІНФОРМАЦІЇ, ЩО ПЕРЕДАЄТЬСЯ ТАЙМЕРНИМИ РОЗРЯДНО-АНАЛОГОВИМИ ОПЕРАНДАМИ ІЗ ЗАХИСТОМ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

05.13.08 — обчислювальні машини, системи, мережі, елементи та пристрої обчислювальної техніки та систем керування

Автореферат дисертації на здобуття наукового ступеня кандидата технічних наук

Київ 1995

Дисертацією є рукопис

Робота виконана в Ін
Національної академі

Науковий керівник: доктор технічних наук, професор
БАРДАЧЕНКО Віталій Феодосійович,

Офіційні опоненти: доктор технічних наук
РОМАНОВ Володимир Олександрович
кандидат технічних наук
КОСМАЧ Юлій Петрович.

Провідна організація: ВО «Електронмаш», м. Київ.

Захист відбудеться «30» XI 1995 на засіданні Спеціалізованої Вченої ради Д 01.39.04 при Інституті кібернетики ім. В. М. Глушкова НАН України за адресою:
252022, Київ 22, проспект Академіка Глушкова, 40.

З дисертацією можна ознайомитися у науково-технічному архіві інституту.

Автореферат розісланий «26» жовтня 1995 р.

Учений секретар
Спеціалізованої Вченої ради
ГУМЕНЮК-СИЧЕВСЬКИЙ В. І.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

АКТУАЛЬНІСТЬ ПРОБЛЕМИ. Здійснюваний у останній час інтенсивний розвиток обчислювальної техніки, засобів обробки та передачі інформації на основі новітніх науково-технічних досягнень мікроелектроніки та мікропроцесорної техніки призвело до появи обчислювальних систем на основі мікропроцесорів і створення багатопроцесорних однорідних обчислювальних структур (БООС) із паралельною обробкою інформації. Значний внесок в розвиток цього напряму було зроблено відомими вченими Б.М. Глушковим, В.С. Михалевичем, О.В.Палагіним. Це дозволило при розв'язанні певного класу задач істотно підвищити швидкодію у порівнянні із однопроцесорними універсальними ЕОМ. Використання багатопроцесорних обчислювальних структур у складі систем автоматичного управління передбачає можливість обробки інформації із численних різнорідних датчиків у реальному масштабі часу. Ці питання плодотворно розвинуті провідними вченими Б.М. Малиновським, А.І. Кондалевим, В.О. Романовим, В.А. Фабричевим.

Ускладнення системи за рахунок включення у неї великої кількості аналогово-цифрових перетворювачів призводить до необхідності утворення гібридних БООС.

У працях Г.Є. Пухова, В. Ф.Бардаченко, Ю.В.Корольова запропонований принципово новий підхід до побудови гібридних обчислювальних засобів, оснований на виконанні групової математичної операції скалярного добутку векторів з допомогою обчислювальних пристроїв, часозадаючими елементами яких є аналогові R, C - датчики або дискретно-керовані RC-ланцюги.Такі обчислювальні пристрої одержали назву таймерних за аналогією із таймерами, у яких у вигляді часозадаючих елементів використовуються аналогові RL, RC-ланцюги.Операційним параметром таймерних обчислювальних пристроїв є не струм чи напруга, а час.

Одним із перспективних напрямків оптимізації основних показників обробки і передачі інформації у БООС є розробка теорії розрядно -аналогових обчислювальних систем, чималий вклад у яку внесено у працях Г.Є. Пухова, В.Ф. Євдокімова, В.Ф.Бардаченко, Ю. В. Корольова. Застосування цієї теорії до таймерних принципів обробки інформації зумовило розвиток принципово нового напрямку : таймерних розрядно-аналогових обчислювальних пристроїв та систем.

МЕТОЮ РОБОТИ є дослідження принципів обробки та передачі інформації з допомогою таймерних розрядно-аналогових операндів із захистом від несанкціонованого доступу.

ЗАДАЧІ ДОСЛІДЖЕНЬ. В роботі вирішуються такі задачі:

1. Дослідження принципів функціонування таймерних обчислювальних пристроїв та засоби підвищення їх ефективності.

2. Дослідження принципів подання таймерної інформації у розрядно-аналоговій формі.

3. Аналіз існуючих засобів і алгоритмів захисту інформації від несанкціонованого доступу.

4. Розробка принципів обробки та передачі інформації таймерними розрядно-аналоговими операндами із захистом від несанкціонованого доступу та побудову математичної моделі пропонованого способу захисту.

5. Розробка і обґрунтування якісних і кількісних характеристик подання інформації у розрядно-аналоговій формі.

6. Розробка методики розрахунку імовірносних характеристик пропонованого способу маскування інформації і її застосування на конкретних прикладах.

7. Розробка алгоритмів опрацювання інформації на таймерних обчислювальних пристроях.

МЕТОДИ ДОСЛІДЖЕНЬ основані на теоретичних основах обчислювальної техніки, теорії імовірностей, лінійній алгебрі, теорії інформації, математичному моделюванні об'єктів обчислювальної техніки.

НАУКОВА НОВИЗНА. В роботі здобуті такі результати:

- в результаті проведених досліджень вирішена задача розробки принципів опрацювання і передачі інформації таймерними розрядно-аналоговими операндами із захистом від несанкціонованого доступу;

- проведена якісна оцінка подання таймерної інформації у розрядно-аналоговій формі і обґрунтовано найбільш доцільне розбиття таймерного операнда з точки зору цієї характеристики;

- на основі розроблених принципів захисту побудована математична модель способу маскування таймерної інформації;

- розроблена методика розрахунку імовірносних характеристик описаного способу захисту інформації, наведено результати застосування цієї методики на конкретних прикладах;

- розроблені алгоритми опрацювання інформації, орієнтовані

на використання таймерних обчислювальних пристроїв;

– розроблені засоби підвищення ефективності опрацювання інформації на таймерних обчислювальних пристроях.

ДОСТОВІРНІСТЬ досліджень підтверджена обчислювальними експериментами над моделями на ПЕОМ, розробленими дослідними зразками ТРАП та таймерного маскиратору, які підтвердили працездатність запропонованих принципів.

ПРАКТИЧНА ЦІННІСТЬ. Розроблені принципи опрацювання і передачі інформації із захистом від несанкціонованого доступу дозволяють по-новому підійти до проблеми створення багатопроцесорних обчислювальних структур гібридного типу у складі систем автоматичного керування із паралельною обробкою інформації. Застосування розроблених принципів обробки інформації дозволяє підвищити надійність та ефективність обміну інформацією, скоротити час розв'язку задач керування, обробки сигналів та інших.

Автор приймав участь у виконанні договорів за даною тематикою на протязі 1985– 1993 років із Інститутом проблем моделювання в енергетиці НАН України, Всесоюзним науково-дослідним інститутом систем керування і зв'язку (м. Москва), Інститутом кібернетики ім. В.М.Глушкова НАН України, Фізико-механічним інститутом НАН України (м.Львів), ВО "Електронмаш", м. Київ.

ВИКОРИСТАННЯ У ПРОМИСЛОВОСТІ. Наукові результати роботи використані у НДІ "Прогрес", м. Москва при проектуванні ВІС ТРАП на базі БМК "1515 ХМ1"; на ВО "Електронмаш", м. Київ, де виготовлено 5 дослідних зразків телефонного маскиратора "Кримтел", і на 1996 р. планується його серійний випуск; на НВО "Квазар", м.Москва, при виготовленні дисплейних класів "Квазар".

АПРОБАЦІЯ РОБОТИ. Основні результати роботи доповідались на : III науково-технічній конференції "Проблеми надійності електротехніки" (м. Черкаси, 1988 р.), науково-технічній конференції "Проблеми, методи, досвід розробки АСУЗ" (м. Москва, 1990 р), наукових семінарах "Проблеми аналізу і забезпечення точності систем моделювання і управління" відділу моделювання динамічних систем ІПМЕ НАН України та "Таймерні розрядно-аналогові обчислювальні пристрої і системи" відділу таймерних обчислювальних пристроїв ІК НАН України.

ПУБЛІКАЦІЇ. Матеріали дисертації знайшли своє відображення у десяти друкованих працях.

СТРУКТУРА ТА ОБСЯГ ПРАЦІ. Дисертація виконана на 111 сто-

рінках машинописного тексту, містить 7 рисунків та складається із вступу, чотирьох розділів, висновків, списку літератури, що містить 53 праці, та 2 додатків.

ЗМІСТ РОБОТИ

У ВСТУПІ дається обґрунтування актуальності праці, формулюється її мета та основні положення, що представлені до захисту.

ПЕРШИЙ РОЗДІЛ присвячено аналізу обчислювальних пристроїв (ОП) з імпульсною формою вхідної, проміжної та вихідної інформації. Відповідно до використання одного із цих параметрів, ОП можна поділити на ОП із амплітудно-імпульсною модуляцією, ОП із частотно-імпульсною модуляцією, ОП із фазо-імпульсною модуляцією і ОП із часо-імпульсною модуляцією.

Одним із різновидів зазначених ОП є формувачі інтервалів часу аналогового та гібридного типу на базі таймерів із часозадаючими RC - і RL- ланцюгами, що дістали назву таймерних обчислювальних пристроїв (ТОП). Такі ОП можуть виконувати набір самих різних по функціональному призначенню керуючих, контрольно-вимірювальних, обчислювальних й логічних операцій із вхідними операндами як : генерацію імпульсів у широкому діапазоні тривалостей, сумування тривалостей імпульсів, аналого - цифрові перетворення, підтримання у заданих межах змінних та контрольованих параметрів та інше. Вони можуть використовуватися у вигляді елементарних таймерних процесорів (ЕТП) таймерних однорідних обчислювальних структур.

Одним із недоліків розглянутих ТОП є оперування із повнорозрядним операндами, що знижує ефективність їх використання в обчислювальних процесах внаслідок недостатньої точності обчислень та швидкості обробки інформації. Тому були запропоновані засоби підвищення продуктивності ТОП з використанням розрядно-аналогових принципів обробки інформації. В даному розділі зроблено аналіз проведених досліджень і одержаних результатів, розглянуто де-які основні напрямки розвитку ТОП із розрядно-аналоговою формою подання операндів. Так, наслідком розвитку цих ідей стали розробка таймерного пристрою введення, передачі та обробки інформації і виготовлення на його базі дисплейного класу принципово нової конструкції, розробка вимірювально-обчислювальних систем, системи технічного зору таймерного типу, пристрою для медичної експрес-діагностики та ін.

Одним із найважливіших напрямків розвитку цих ідей стало опрацювання принципів побудови таймерних розрядно-аналогових процесорів (ТРАП), що ,реалізують групову операцію скалярного добутку векторів великої розмірності. Перспективним напрямком є застосування ТРАП у вигляді співпроцесорів універсальних ЕОМ. Це дозволяє підвищити продуктивність таких ЕОМ на векторно-матричних операціях. На підставі проведених досліджень автором зроблено висновок, що використання ТРАП викликає необхідність розробки спеціальних алгоритмів,основною операцією в яких буде операція скалярного добутку векторів.

Ще одним перспективним напрямком стала розробка і реалізація на базі зазначених ТОП таймерних постійних запам'ятовуючих пристроїв (ТПЗП), призначених для тривалого зберігання і обробки незмінної в процесі роботи ЕОМ інформації на основі опрацювання таймерних операндів, що формуються за допомогою часозадаючих RC-ланцюгів.

У процесі обробки та передачі інформації значне місце посідає дослідження впливу різноманітних дестабілізуючих чинників на операнд, що передається. Застосування розрядно-аналогового розбиття операндів дозволяє значно підвищити толерантність обробки і передачі інформації. Слід зауважити, що ці питання ще недостатньо досліджені в літературних джерелах, деякі висновки і твердження потребують чіткого доведення.

Особлива увага останнім часом приділяється проблемі захисту інформації від несанкціонованого доступу, причому об'єктами нападу зловмисників все частіше стають не лише системи опрацювання даних спеціального призначення, але і комерційні системи. Враховуючи сучасні темпи розвитку обчислювальної техніки , можна зробити висновок, що традиційних засобів захисту інформації недостатньо для надійного її закриття.

Ця проблема є актуальною і для інформаційно-обчислювальних систем опрацювання даних таймерного типу. Це питання в літературі поки що недостатньо висвітлене.

ДРУГИЙ РОЗДІЛ присвячено питанню дослідження стійкості до дестабілізуючих чинників таймерних операндів у розрядно-аналоговій формі. Наведена теоретична основа апарату розрядних перетворень. Підкреслено позитивні особливості кодування інформації таймерними операндами, серед яких основними є наступні :

- на відміну від від класичних систем передачі даних канал зв'язку на час передачі інформаційної частини коду не займається; старт-стопні службові імпульси визначають тривалість таймерного операнду, тому при рівних умовах приймому службових імпульсів досягається більш висока завадозахищеність по порівнянню з традиційними засобами передачі даних, при яких кодова комбінація символів підлягає різноманітним спотворенням ;
- таймерний операнд дозволяє багатократне тиражування без зміни самого операнду.

Далі розглянуті питання, пов'язані з толерантністю обробки і передачі інформації в ТОП.

Запровадимо міру втрати інформації, що передається таймерними операндами. Якщо внаслідок будь-якого дестабілізуючого чинника спотворений n-й розряд N-розрядної послідовності імпульсів, ця міра складе

$$P(n) = \frac{2^{n-1}}{2^N - 1}, \qquad (1)$$

При передачі тієї ж інформації в розрядно-аналоговій формі (s груп по k розрядів в групі, група старших розрядів може бути неповною), при втраті імпульса в m-й групі міра складе

$$P1(m) = \frac{2^{k(m-1)}}{2^N - 1}, \qquad (2)$$

де

$$s = \begin{cases} [N/k] + 1, & \text{якщо } N \text{ не є кратним до } k \\ N/k. & \text{інакше.} \end{cases}$$

Довжина імпульсної послідовності при цьому збільшиться в

$$T(k) = \frac{(2^k - 1)\, s}{N}. \qquad (3)$$

Для оцінки ефективності подання операндів в розрядно-

аналоговій формі запроваджений коефіцієнт толерантності розрядно-аналогового розбиття T1(k), що пропорційний відношенню відповідних значень P при спотворенні імпульса старшого розряду повнорозрядного подання інформації та P1 при спотворенні в групі старших розрядів, і обернено пропорційний коефіцієнту збільшення довжини імпульсної послідовності τ :

$$T1(k) = \frac{P(N)}{P1(s)\ T(k)} . \qquad (4)$$

Коефіцієнт толерантності характеризує стійкість до спотворення імпульсів в групі старших розрядів.

В роботі досліджена залежність T1 від k. Показано, що в разі розбиття операнду на повні групи (тобто коли група старших розрядів є повною), T1 приймає вигляд

$$T1(k) = \frac{2^{k-1}\ k}{2^k - 1}, \qquad (5)$$

і зростає із збільшенням k по закону, близькому до лінійного. У випадку k = 1 (що визначає мінімальну довжину групи) значення T1 = 1. В інших випадках не завжди розбиття дає позитивний ефект. Так, поклавши N = k(s - 1) + r, де 0 < r < k, отримаємо :

$$T1(k) = \frac{r - 1 + \log\left[\frac{Nk}{N-r+k}\right]}{2^k - 1} . \qquad (6)$$

Очевидно, що коефіцієнт толерантності буде більше 1 при виконанні умови

$$r - 1 + \log\left[\frac{Nk}{N-r+k}\right] - k > 0.$$

Опираючись на проведені дослідження, зроблено висновок про те, що найбільш доцільними є розбиття на повні групи. В роботі наведено доказ цього твердження. Показано, що серед поділів на повні групи з точки зору запропонованої характеристики найбільш доцільними є поділи на групи на 2 або на 4 розряди. Цей результат підтверджує зроблені раніше висновки про доцільність саме такого розбиття таймерного операнду.

Далі розглянуто порівняння втрат для звичайного способу передачі інформації і у випадку розрядно-аналогового розбиття операндів. Показано, що втрати для розрядно-аналогових операндів будуть меншими. Аналогічні результати одержані для випадку двох одиночних завад та пакету помилок. При цьому відмічено, що втрати будуть меншими у тому випадку, коли завади припадуть на одну групу.

На підставі проведених досліджень наведено графік залежності коефіцієнта Т1 від довжини групи k для розбиття на повні групи і графік залежності коефіцієнта Т1 від довжини групи k для всіх значень k при N = 32. Використовуючи одержані вище результати, обґрунтовано зниження коефіцієнта толерантності Т1 при розбитті з неповною групою старших розрядів. Також пояснюється стрибковий характер зміни значень Т1 для розбиття з неповною групою старших розрядів .

Третій розділ присвячено виробленню концепції захисту інформації, що передається таймерними розрядно-аналоговими операндами. Спочатку дається стислий огляд традиційних систем захисту. Показано, що проблема захисту уже багато років знаходиться в центрі уваги не тільки фахівців, але і широкого кола користувачів, причому особлива увага приділяється небезпеці несанкціонованого (випадкового чи злоумисного) одержання інформації особами, для яких вона не призначалась. Ця небезпека стала настільки гострою, що традиційні засоби, що існували раніше, у докомп'ютерну епоху, виявилися недостатніми. Тому наявність механізмів захисту (як апаратних, так і програмних) є одним із обов'язкових вимог при проектуванні систем обробки даних.

Шифрування чи криптографічне перетворення інформації по визнанню зарубіжних фахівців є найбільш універсальним засобом захисту, хоч практична реалізація алгоритмів шифрування сполучена з подоланням значних труднощів. Далі в роботі розглянуто основні підходи до шифрування: використання гами шифру за допомогою датчика псевдовипадкових чисел; використання підстановки (одного знакового ряду замість іншого), перестановки (зміна порядку слідування знаків у вихідному тексті) і доповнення (алгебраїчна комбінація знаків тексту із знаками "ключа ").

Враховуючи, що маскування - один з найважливіших засобів захисту інформації шляхом її криптографічного закриття і той фактор, що таймерні операнди, які передаються в розрядно-ана-

логовой формі,мають високу стійкість до впливу різноманітного роду дестабілізучих чинників і це дозволяє вважати їх підхожими для надійної передачі інформації, пропонується концепція захисту інформації від несанкціонованого доступу.

Нехай N-розрядний таймерний операнд, що передається, представлено в розрядно-аналоговій формі і складається з S груп по k розрядів в групі (розбиття вважається на повні групи). Маскування відбувається за двома функціями: F і μ.При надходженні операнду на комутатор функції μ відбувається перестановка місцями (або перестановка по черговості, в залежності від того, як передаються таймерні операнди, паралельно чи послідовно) інтервалів часу по де-якому випадковому закону . Після цього "перемішаний" операнд поступає на комутатор функції F, де також по випадковому закону відбувається зміна тривалостей інтервалів часу. Таким чином, в лінію зв'язку будуть поступати таймерні операнди, що маскувалися по функціям μ і F. На приймному кінці лінії зв'язку будуть розмасковані за допомогою аналогічного приймному комутатора функції μ і декодера функції F.

Дана концепція захисту інформації може використовуватися при побудові таймерних постійних запам'ятовуючих пристроїв (ТПЗП) із захистом від несанкціонованого доступу, а також при обміні комерційною інформацією між різними абонентами у інформаційно-обчислювальних мережах таймерного типу. Основними завданнями, що вирішуються при цьому, є запобігання розкриття змісту і детального аналізу інформації, а також заборона несанкціонованого впливу на інформацію.

Для опису математичної моделі засобу захисту інформації, що пропонується, покладемо, що N=8, тобто операнди ,які передаються,є 8-розрядними. Це відповідає стандартному коду одного символа. При цьому покладемо, k=2, тобто 8-бітовий операнд представлений в розрядно-аналоговій формі у вигляді послідовності із 4-х груп по 2 розряда в групі. Уведемо такі позначення :

а) нехай Г - множина усіх комбінацій довжини 2 із 0 і 1, що називаються далі "двійками",тобто Г = {00,01,10,11};

б) нехай $\alpha, \beta, \gamma, \delta$ - елементи Г, причому завжди різні, тобто $\alpha \neq \beta \neq \gamma \neq \delta$;*

в) нехай n_1, n_2, n_3, n_4 - номери "двійок" відпові-

дного двійкового подання коду символу, що передається, після впливу на нього функції μ.

Тоді маскування символів, що передаються, описується підстановкою

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 \\ n_1 & n_2 & n_3 & n_4 \end{pmatrix} . \qquad (7)$$

Цією підстановкою встановлюється відповідність між прообразом (символом, що передається) і образом (символом, що замаскований). Оскільки всіх таких підстановок буде 24, то кожному образу може відповідати один із 24 (не обов'язково різномантітних) прообразів. Всі прообрази можна розподілити на множини, що характеризуються тією властивістю, що кожному елементу такої множини відповідає образ із тієї ж множини. Кількість елементів множини будемо називати довжиною множини. В роботі побудовано таблиці розподілу довжин по множинам для 8-бітових і 16-бітових образів.

Нехай в повідомленні довжини N1 було s_i елементів із кожного набору для 8-розрядних образів, $i = 1..5$.

Однією із характеристик, притаманних для будь-якого засобу маскування, є кількість K1 всіх можливих повідомлень із елементів множин, яким належать відповідні образи. Ця кількість в даному випадку складе

$$K1 = 2^{2s_2+s_3+2s_4+3s_5+(s_3+s_4+s_5)\log 3} . \qquad (8)$$

В частковому випадку, при передачі текстової інформації, і враховуючи, що не всі прообрази можуть бути задіяні для передачі інформації, можна підібрати кодову таблицю символів таким чином, щоб коди образів, що зустрічаються в повідомленні, вдучали на множини з найбільшою довжиною, тобто на множини із 4 і 5 наборів. Значення величини K1 в такому випадку складе

$$K1 = 12^{N1} * 2^{s_5} , \qquad (9)$$

де s_5 - кількість символів із п'ятого набору.

Розглянемо механізм маскування таймерних операндів за допомогою функції P, залишивши в силі зроблені раніше припущення. Функцію P далі називатимемо функцією деформації, а її

значення - коефіцієнтами деформації.

Для цього уведемо слідуючі позначення :

τ_1 - таймерний розрядно-аналоговий операнд, що надходить із виходу комутатора функції μ на вхід кодера функції F;*

τ_2 - таймерний розрядно-аналоговий операнд, що надходить із виходу кодера функції F в лінію зв'язку;

КF - упорядкована множина із L значень, що може коефіцієнт деформації функції F :

k_1 - i-тий елемент із КF, i=1.. L.

Дія функції F полягає в зміні тривалостей операндів τ_1 , що передаються, в k_1 раз, тобто

$$\tau_2 = k_1 * \tau_1 \quad . \qquad (10)$$

Зауважимо, що наведена концепція захисту інформації не вступає у протиріччя із відомими схемами захисту інформації. Тому існує можливість використати їх у сукупності із наведеним методом для більш надійного захисту інформації.

Далі автором наведено розрахунки ймовірносних характеристик запропонованого способу захисту інформації. Ці характеристики дозволяють якісно оцінити дану концепцію маскування. На основі запроваджених характеристик автором запропоновано методику, яка дозволяє зробити якісну оцінку маскування за наведеною концепцією для різних типів поділу операндів на розрядні групи і різних систем коефіцієнтів деформації. По наведеній методиці зроблено розрахунки для одного прикладу розрядного розбиття (8-розрядного операнду на групи по 2 розряди), часткових значень вхідних тривалостей τ_1 і часткової системи коефіцієнтів деформації.Розраховані оцінки дозволяють зробити висновки про якість маскування для цього випадку. Так, ймовірність того, що операнд додатково не буде маскований функцією F внаслідок невдалого сполучення вхідного операнда і коефіцієнта деформації складе

$$P(A) = 0.0002 \quad . \qquad (11)$$

Це говорить про те, що лише 2 символи з 10000 не будуть додатково масковані функцією F. Помітимо, що для іншої системи коефіцієнтів деформації це значення може бути іншим. Питання знаходження більш вдалої з точки зору наведеної методики системи

коефіцієнтів деформації в дисертації не досліджувалося.

Далі обчислена ймовірність демаскування операнда, маскованого лише функцією F

$$P(C_{заг}) \approx 0{,}023 \qquad (12)$$

і маскованого лише функцією μ

$$P(D) = 0{,}16 . \qquad (13)$$

В розділі 4 наведено де-які алгоритми опрацювання інформації на таймерних обчислювальних пристроях. Так, враховуючи ефективність використання ТРАПа, при розв'язуванні задач постала необхідність в застосуванні алгоритмів, в яких основну частину обчислень займає операція скалярного добутку векторів і що найбільш вільні від виконання інших операцій. Даний розділ присвячений вибору алгоритмів для розв'язання таких поширених задач лінійної алгебри як знаходження оберненої матриці і знаходження власних значень симетричної матриці.

Розглянемо першу із зазначених вище задач. Нехай маємо квадратну матрицю A вимірності $n \times n$. Суть способу, що пропонується, полягає в зведенні вихідної матриці A до одиничної E шляхом послідовного множення її на матриці спеціального виду, що легко будуються і що мають схожу структуру.

На першому кроці останній стовпець $(a_{1n}\ a_{2n}\ \dots\ a_{nn})^T$ матриці A перетвориться в стовпець $(0\ 0\dots\ 0\ 1)^T$. Це досягається шляхом множення її ліворуч на матрицю M_n виду

$$M_n = \begin{vmatrix} 1 & 0 & \dots & 0 & -\frac{a_{1n}}{a_{nn}} \\ 0 & 1 & \dots & 0 & -\frac{a_{2n}}{a_{nn}} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 1 & -\frac{a_{n-1,n}}{a_{nn}} \\ 0 & 0 & \dots & 0 & \frac{1}{a_{nn}} \end{vmatrix} . \qquad (14)$$

В результаті одержуємо матрицю $A_1 = M_n A$ і матрицю $E_1 = M_n E$, де E – одинична матриця. Продовжуючи це процес, через n кроків одержимо

$$A_n = E = M_1 (M_2 \dots (M_n A)\dots).$$
$$E_n = M_1 (M_2 \dots (M_n E)\dots). \qquad (15)$$

Звідси, враховуючи асоціативність добутку матриць, остаточно одержимо

$$A^{-1} = M_1 M_2 \dots M_n . \qquad (16)$$

Порівняльний аналіз швидкодії розв'язання цієї задачі на ПЕОМ із використанням ТРАПа показав, що для обернення матриці вимірності 20×20 по наведеному вище алгоритму витрачається в 1,6 раз менше часу, ніж для розв'язання того ж завдання на ПЕОМ без співпроцесора.

Даний алгоритм пропонується використати для розв'язання завдання керування фазованими антенними решітками на обчислювальному комплексі, який використовує у вигляді акселератору таймерний розрядно-аналоговий процесор.

Далі розглянуто алгоритм знаходження власних значень симетричних матриць. Для розв'язання цієї задачі на таймерних обчислювальних пристроях пропонується комбінований спосіб, що полягає в знаходженні власних значеннь через використання коефіцієнтів відповідного характеристичного многочлена і зведенні практично всіх обчислень до матрично-векторних операцій. В його основі лежить зведення вихідної матриці A до виду Фробеніуса

$$\begin{vmatrix} P_1 & P_2 & \dots & P_{n-1} & P_n \\ 1 & 0 & \dots & 0 & 0 \\ & \cdot & \cdot & \cdot & \\ 0 & 0 & & 1 & 0 \end{vmatrix} . \qquad (17)$$

де p_i , $i=1 .. n$, - коефіцієнти характеристичного многочлена

$$D(\lambda) = \lambda^n - p_1\lambda^{n-1} - \dots - p_n . \qquad (18)$$

Нехай λ_n - найбільше за модулем власне значення вихідної матриці. Враховуючи відносну малість по порівнянню із λ_n інших λ_i, одержимо

$$\lambda_n \approx \frac{Sp\ A^{m+1}}{Sp\ A^m} , \qquad (19)$$

де Sp A - слід матриці A, m -натуральне число

Знаючи один корінь характеристичного многочлена, можна розкласти його на множники :

$$D(\lambda) = (\lambda - \lambda_n)(\lambda^{n-1} - p_1'\lambda^{n-2} - \dots - p_{n-1}'), \qquad (20)$$

де p_i' визначаються за формулами

$$p_i' = p_i + \lambda_n p_{i-1}' , \quad i = 1.. n-1 ,$$
$$p_0' = 1 \qquad (21)$$

Помітимо, що многочлен $D'(\lambda) = \lambda^{n-1} - p_1'\lambda^{n-2} - \dots - p_n'$ є характеристичним для деякої матриці A' виду (18), що має вимірність на одиницю меншу. Отже, для матриці A' можливо за формулою (20) знайти найбільше за модулем власне значення, що буде другим власним значенням вихідної матриці A. Продовжуючи цей процес,можна обчислити всі власні значення матриці A.

В роботі наведено оцінки похибки даного методу обчислень.

Останній параграф розділу присвячений питанню підвищення продуктивності ТРАП. В дисертації розглянуто два способи підвищення продуктивності ТРАП, що використовують шлях удосконалення алгоритмів обчислення.

Першим способом підвищення продуктивності ТРАП є оптимізація алгоритму обчислення скалярного добутку. Для здобутку цієї мети розглянуто алгоритм Винограда. Його застосування до алгоритму обчислення добутку матриць дозволяє зменшити кіль-

кість операцій множення майже вдвічі.

Іншим способом підвищення ефективності обчислень є розбиття вихідних матриць на клітини. Кількість парних добутків у цьому випадку зменшиться у 2,5 раз у порівнянні із звичайним способом множення матриць. Застосовуючи обидва описаних способи у сукупності, можна значно скоротити час розв'язку задач векторної алгебри на ТРАП.

У ВИСНОВКАХ формулюються основні результати роботи.

У ДОДАТКУ 1 наведено програмну модель описаного способу маскування і таблицю розподілу образів для 8-бітових блоків.

У ДОДАТКУ 2 наведено програмну модель пропонованого способу знаходження власних значень симетричної матриці.

ОСНОВНІ РЕЗУЛЬТАТИ РОБОТИ можуть бути сформульовані таким чином:

1. В результаті проведених досліджень розроблені принципи опрацювання і передачі інформації таймерними розрядно-аналоговими операндами із захистом від несанкціонованого доступу. Маскування реалізується комплексно за допомогою перестановочної функції μ і функції деформації F.

2. Показано, що результат функція маскування не залежить від порядку їх дії. При цьому описані функції не вступають у протиріччя із існуючими механізмами захисту і можуть бути використані у комплексі із ними з метою більш надійного захисту.

3. Розроблена методика розрахунку імовірносних характеристик запропонованого способу захисту і наведені результати її застосування на конкретних прикладах.

4. На основі запропонованих принципів опрацювання інформації розроблені дисплейні класи нової конструкції, ВІС таймерного розрядно-аналогового процесора на базі БМК "1515 ХМ1", таймерний маскиратор "Криптел".

5. Проведена якісна оцінка подання таймерної інформації у розрядно-аналоговій формі і обґрунтовано найдоцільніше розбиття таймерного операнда з точки зору цієї характеристики.

6. Побудована математична модель розробленого способу маскування таймерної інформації.

7. Запропоновані алгоритми опрацювання інформації, орієнтовані на використання таймерних обчислювальних пристроїв.

8. Запропоновані засоби підвищення ефективності опрацюван-

ня інформації на таймерних обчислювальних пристроях.

ПУБЛІКАЦІЇ ПО ТЕМІ ДИСЕРТАЦІЇ

1. Бардаченко П.М., Григорук П.М. К оценке эффективности вычислений клеточным методом на скаляторах. -Электрон. моделирование, 1987.-№ 4.-с 103-104.

2. Бардаченко В.Ф., Григорук П.М. О моделировании одного метода решения задачи нахождения собственных значений на скаляторах.//Техника средств связи. -Сер.СС.-1988.-Вып.1.-с 52-56

3. Бардаченко В.Ф., Григорук П.М. Оценка толерантности обработки и передачи сигналов в вычислительных комплексах таймерного типа.-Тезисы докладов III науч.-техн. конференции "Проблемы, методы, опыт создания АСУС". - Москва.- 1990.-с 60-61.

4. Григорук П.М, Радельчук Г.И. Обращение матрицы на ПЭВМ с таймерным разрядно-аналоговым скаляторным процессором.//Техника средств связи.-Сер. СС.-1989.-Вып.2.- с 54-58.

5. Бардаченко В.Ф.,Григорук П.М., Герасимчук А.М. Система технического зрения таймерного типа для визуального контроля в РТК.- Тезисы докладов науч.-техн. конференции "Роботизация и ГАП",-вып.3.-1986.-с 111.

6. Бардаченко В.Ф., Григорук П.М., Гаврилова А.С. Реализация одного алгоритма управления фазированной антенной решеткой с помощью функционально-ориентированного комплекса на базе ПЭВМ и скаляторного процессора. -Тезисы докладов III науч.- техн. конференции "Проблемы нелинейной электротехники" ,- ч.2.-Киев.-1988.-с 67-70.

7. Бардаченко В.Ф., Григорук П.М., Шурчков И.О. Принципы маскирования коммерческой информации, передаваемой таймерными операндами.// Техника средств связи. -Сер. СС.- 1991.-с 31-34.

8. Разработка таймерных вычислительных устройств систем автоматизации управления и информатики.-Отчет по НИР "Высокопроизводительные ПЭВМ и проблемно-ориентированные комплексы".- Киев,1988.

9. П.М. Григорук. Методика розрахунку імовірносних характеристик маскування таймерної інформації.-Тези доповідей науково-практичної конференції з нагоди презентації технологічного Університету Поділля.- Хмельницький, 1994.

10. П.М.Григорук. Спосіб підвищення продуктивності ТРАП.- Тези доповідей конф."Застосування математичного моделювання та математичних методів в наукових дослідженнях",Львів , 1994.

Анотація

Григорук Павло Михайлович. Принципи обробки інформації, що передається таймерними розрядно-аналоговими операндами із захистом від несанкціонованого доступа. Дисертація на здобуття вченого ступеню кандидата технічних наук із спеціальності 05.13.08 «Очислювальні машини, системи, мережі, елементи та пристрої обчислювальної техніки та систем керування».

Інститут кібернетики НАН України, 1995 р.

Дисертація містить теоретичні дослідження в галузі захисту інформації в таймерних розрядно-аналогових пристроях. Запропонований спосіб захисту інформації, побудовано його математичну модель, розраховано ймовірносні характеристики. Розглянуто алгоритми опрацювання інформації на таймерних розрядно-аналогових пристроях.

Ключові слова: несанкціонований доступ, захист інформації, таймерний розрядно-аналоговий операнд, маскування інформації.

Annotation

Grigoruk Pavlo Mikhajlovich. The principles of information processing which transmits by the timer bit-slice-analogical operands with fetch protect. This thesis is written to assign the degree of Candidate of Technical Sciences on the speciality 05.13.08 «Computers, systems, nets, elements and devices of computers and management systems».

The Institute of Cybernetics NAS of Ukraine, 1995.

The thesis deals with the theoretical investigations in the area of informations protect in the timer bit-slice-analogical devices. The way of information protect was proposed, its mathematical model was worked out and some characteristics were counted. Also the thesis deals with the algorithm of information processing on the timer bit-slice-analogical devices.