Науковий журнал 3.2007

ВІСНИК

Хмельницького національного університету

Том 1

Технічні науки

ВІСНИК
Хмельницького
національного
університету

Засновано в липні 1997р. ***Виходить 6 разів на рік***

Хмельницький, 2007, №3, Т.1 (93)

Засновник і видавець: Хмельницький національний університет
(до 2005 р. – Технологічний університет Поділля, м. Хмельницький)

Відповідальний за випуск: д.т.н., професор Локазюк В.М.

Технічний редактор Горященко К.Л.
Редактор-коректор Броженко В.О.

Адреса редакції: **Україна, 29016,**
м. Хмельницький, вул. Інститутська, 11,
Хмельницький національний університет
редакція журналу "Вісник Хмельницького національного університету"

☎ **(8-03822) 2-51-08**

e-mail: **patent_1@beta.tup.km.ua**

web: **http://visniktup.narod.ru** **http://vestnik.ho.com.ua**
http://library.tup.km.ua/visnyk_tup.htm

Зареєстровано Міністерством України у справах преси та інформації.
Свідоцтво про державну реєстрацію друкованого засобу масової інформації
Серія КВ № 9722 від 29 березня 2005 року (перереєстровано)
Бюлетень ВАК №2, 2006

СПЕЦІАЛІЗОВАНІ КОМП'ЮТЕРНІ СИСТЕМИ

$$S_1 = \sum x_{ij} \forall i + j = 2n;$$
$$S_2 = \sum x_{ij} \forall i + j = 2n - 1;$$
$$S_3 = \sum x_{ij} \forall i + j = 2n - 2;$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$S_n = \sum x_{ij} \forall i + j = 2;$$

де S_n – розряди векторного представлення числа А.

Представлені вирази переходу від векторного представлення до матричного і зворотне перетворення показує простоту цих операцій, що дозволяє легко імплементовувати матричну систему числення в існуючі засоби комп'ютерної техніки.

Висновок

Проведені теоретичні дослідження показують альтернативне представлення кодових базисів у вигляді матричної системи числення, що відкриває перспективи дослідження таких систем числення та пошуку методів їх обробки з покращеними системними характеристиками.

Література

1. Угрюмов Е.П. Цифровая схемотехника. – СПб.: БХВ – Санкт-Петербург, 2000. – 528 с.

2. Николайчук Я., Король Р. Вертикальна інформаційна технологія в базисі Галуа – новий напрямок розвитку комп'ютерних машин. – Львів: ССШ'2000, 254-258 с.

3. Николайчук Я. М., Круцкевич Н.Д. Принципи побудови RCG процесора Тези міжнародної науково-технічної конференції. "Контроль і управління в складних системах" (КУСС – 2003). – Вінниця: «УНІВЕРСУМ – Вінниця». – 2003. – С. 73.

4. Круцкевич Н.Д. Принцип побудови дешифраторів кодів Галуа пам'яті колективного доступу // Вісник Технологічного університету Поділля. Хмельницький, 2004, № 2. – Ч.1, Т2.– С. 113-116.

5. Круцкевич Н.Д. Системні характеристики лічильників в різних теоретикочислових базисах // Вісник національного університету Поділля, Хмельницький, 2005. – Ч.1, Т2. – С. 219-223.

6. Сергиенко А.М. VHDL для проектирования вычислительных устройств. – К.: ЧП. "Корнейчук", ООО "ТИД " ДС, 2003.

7. Суворова Е.А., Шейнин Ю.Е. Проектирование цифровых систем на VHDL. – СПб.: БХВ-Петербург, 2003.

8. Столлингс В. Структурная организация и архитектура компьютеных систем: Пер. с англ. – 5-е изд. Пер. с англ. – М.: Издательський дом "Вильямс", 2002. – 896 с.

Надійшла 26.2.2007 р.

УДК 618.5.01: 614.844

А.А. ТИМЧЕНКО, М.В. ПІДГОРНИЙ, В.П. МЕЛЬНИК
Черкаський державний технологічний університет

ТЕОРЕТИКО МНОЖИННА МОДЕЛЬ СУЧАСНОЇ БАГАТОКОМПОНЕНТНОЇ АВТОМАТИЗОВАНОЇ СИСТЕМИ КЕРУВАННЯ ОПЕРАТИВНИМ ПОЖЕЖОГАСІННЯМ

В статті проведене системне дослідження автоматизованої системи керування оперативним пожежогасінням (АСКОП), запропонована теоретико множинна модель сучасної багатокомпонентної АСКОП.

Вступ. Постановка проблеми. Експлуатація великих промислових підприємств, атомних і теплових електростанцій, ангарів, інтенсифікація технологічних процесів, збільшення енергозабезпечення підприємств, розширення масштабів і сфер використання пожежонебезпечних матеріалів, висока концентрація матеріальних цінностей на обмежених площах виробничих і складських приміщень призводять до неухильного збільшення імовірності виникнення пожежі і відповідно до прямого і непрямого збитку. Крім цього статистика підкреслює, що приблизно 85 % пожеж в Україні відбувається внаслідок недбалості, халатності і недостатньої інформованості людей у тих та інших питаннях пожежної безпеки [1].

У процесі виконання завдання по гасінню пожежі перед підрозділами МНС України виникає необхідність виявлення осередку пожежі, визначенням причини її виникнення, а також постає питання виявлення шляхів поширення вогню, тривалість пожежі, реєстрації інформаційних факторів пожежі (дим, тепло, випромінювання, полум'я й т.п.), які в подальшому дозволять дати точні висновки при розслідуванні

ному пожежі.

Ефективний шлях вирішення даного завдання бачиться в автоматизації і координації всіх етапів наступного процесу; комплексно оцінити й класифікувати об'єкт захисту по пожежній небезпеці; наукове обґрунтування і вибір ресурсів пожежної охорони; системний аналіз функціонування пожежної охорони; наукове дослідження і вибір шляхів рішення виникаючих задач; проектування автоматизованих систем керування оперативним пожежогасінням (АСКОП) для вирішення цих задач; розробка і впровадження АСКОП; їх цільове використання.

Основна частина. Системне дослідження автоматизованих систем пожежогасіння. Більшість систем пожежної сигналізації, які експлуатуються в Україні, так і закордонних, мають радіальну структуру побудови. Така структура виправдана більш простою схемотехнічною реалізацією, що забезпечує однозначність розшифровки виду й адреси повідомлення „тривоги", а також надійністю, що досягається незалежною обробкою сигналів, які надходять із кожного шлейфа. Засоби пожежної сигналізації будуються на сучасній елементній базі – цифрових інтегральних мікросхемах [2]. Перехід на інтегральні мікросхеми, є тільки першим етапом процесу вдосконалювання протипожежного захисту, забезпеченим значним прогресом у розвитку елементної бази радіоелектроніки. Наступним етапом повинен стати перехід на якісно новий щабель удосконалювання засобів протипожежного захисту, що полягає в переході повністю на цифрові методи перетворення й кодування інформації в пожежних сповіщувачах і широкому застосуванні засобів мікропроцесорної й обчислювальної техніки в установках пожежної сигналізації [3].

В області створення контрольного устаткування пожежної сигналізації інтегральні мікросхеми дозволяють значно знизити габарити, масу й споживану потужність, підвищити надійність, забезпечити нові тактико-технічні характеристики. Хоча вартість нового обладнання, виконаного на новій елементній базі – інтегральних мікросхемах – зросла в порівнянні з релейно-контактними системами пожежної сигналізації минулих років, а їхнє технічне обслуговування й ремонт вимагають більше високої кваліфікації обслуговуючого персоналу, підвищення тактико-технічних характеристик нової апаратури пожежної сигналізації компенсує зазначені недоліки й повністю окупає первісні витрати за рахунок значного підвищення надійності таких систем [4].

На думку авторів потрібно переглянути концепцію побудови систем керування оперативним пожежогасінням, і здійснити перехід на повністю цифрові методи обробки й перетворення інформації від засобів виявлення загорянь і використати елементну базу мікросхем великого ступеня інтеграції, мікропроцесорні набори й засоби обчислювальної техніки.

Створені за такою концепцією системи (рис. 1) характеризуватимуться тим, що пожежний сповіщувач, функції якого обмежуються виміром контрольованих параметрів навколишнього середовища й передачею цих даних по каналам зв'язку до пристрою обробки інформації, який використовує оптимальні алгоритми перетворення й оцінки параметрів сигналів, що надходять по декількох каналах зв'язку одночасно [5]. Аналіз інформаційних параметрів сигналів і прийняття необхідних рішень здійснюється в центральному інформаційно-керуючому пристрої обробки даних, що управляється мікропроцесором відповідно до заданої програми. Ідея повністю зосередити функції системи, аналізувати ситуацію й приймати оптимальне в кожному конкретному випадку рішення безпосередньо в командно-обчислювальному комплексі, а не в зонах, що контролюються є перспективною.

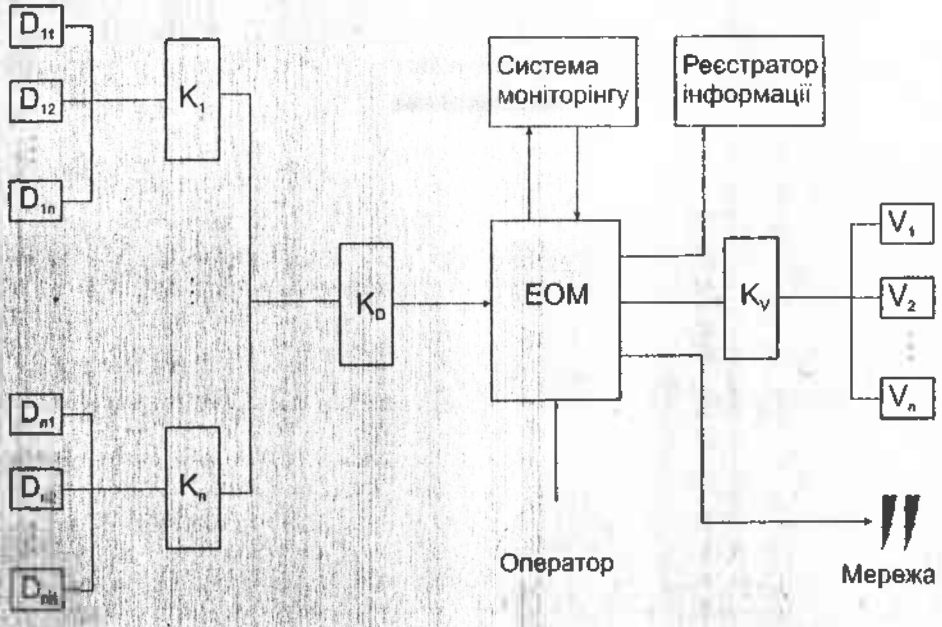

Рис. 1. Структурна схема АСКОП з використанням мережевих технологій

Доручити аналіз пожежонебезпечної ситуації обчислювальному пристрою з метою підвищення

здатності системи до своєчасного й однозначного виявлення пожежонебезпечних ситуацій викли прагненням підвищити вірогідність інформації, звести до мінімуму кількість помилкових сигналів «тривоги» максимально знизити вартість пожежних сповіщувачів, які є найбільш масовою периферійною ланкою систе керування оперативним пожежогасінням, зберегти інформаційні данні про пожежу.

Разом з тим, більше детальний аналіз структури побудови такої системи сигналізації вказує на р труднощів, які є принциповими. Схема сповіщувача повинна містити аналого-цифровий перетворювач, вим до якого по точності перетворення й стабільності його передатної характеристики в процесі експлуата пред'являються досить високі, а також повинен містити пристрій формування коду (умовного номер сповіщувача і передавач інформації (узгоджуючого пристрою). Найбільші технічні труднощі при цьо виникають на ділянках зв'язку між елементами, формуючого повідомлення, і власне ЕОМ, що зв'язан особливостями процесу виникнення, передачі і попередньої обробки даних в автоматизованих систем керування. До цих особливостей відносяться:

- значна розмаїтість периферійної техніки, обумовлена необхідністю обліку як характе виконуваних технологічних операцій, так і людського фактора;
- велика кількість з'єднань (внаслідок чого в ряді випадків витрати на створення каналів зв'яз можуть перевищити вартість автоматизованої системи);
- необхідність захисту переданих і оброблюваних даних від завад (причому вимоги до вірогідно повідомлень, що передаються можуть бути різними для кожного каналу);
- складність самої задачі побудови багаторівневих систем.

З огляду на ці особливості, автори вважає, що гарантоздатна апаратура, яка входить у систему АСКОП повинна мати п'ять рівнів, що відповідають п'ятьом рівням обробки даних на етапах, від місць формуванн повідомлень до введення в АСКОП.

Таблиця 1

Ієрархічна структура моделі багатокомпонентної АСКОП

Рівень ІКС	Компоненти ІКС	Змінна частина компонентів ІКС	Інформація, що обробляється при проектуванні систем и може бути конфігураційно керована
*Level*1			- Склад підсистем, що використовується; - Перелік станів в яких може знаходитися АСКОП.
*Level*2	Множина функціо-нальних підсистем $\{КФП_1,...,КФП_L\}$	Множина функціо-нальних підсистем, що змінюється $\{\Delta КФП\}$	Кількість підсистем АСКОП; Модель надійності АСКОП; Перелік станів в яких може знаходитися функціональна підсистема; Розрахунок показників надійності, оперативної готовності.
*Level*3	Множина блоків $\{КБ_1,...,КБ_M\}$	Множина блоків, що може змінюватися для функціо-нальних підсистем, що змінюється $\{\Delta КБ^{ФП_i}\}$	Кількість блоків, що використовується і кратність резервування для кожного з них Розрахунок показників надійності, оперативної готовності.
*Level*4	Множина функціональних вузлів блоків $\{КФВ_1,...,КФВ_N\}$	Множина функціональних вузлів, що може змінюватися для кожного з блоків $\{\Delta КФВ^{ФБ_i}\}$	Кількість функціональних вузлів, що використовується і кратність резервування для кожного з них Розрахунок показників надійності, оперативної готовності.
*Level*5	Множина елементів $\{КЕ_1,...,КЕ_P\}$	Множина елементів, що може змінюватися для кожного з функціо-нальних вузлів $\{\Delta КЕ^{ФУ_i}\}$	Кількість елементів, що використовується і кратність резервування для кожного з них Розрахунок показників надійності, оперативної готовності.

Структура сучасної багатокомпонентної АСКОП, а також її зміни (еволюція) описуються теоретик множинною моделлю (таблиця 1), відповідно до якої АСКОП складається з множини ієрархічн взаємозалежних рівнів $Level = \{Level1,...,Level5\}$. На кожному i-му рівні формується множин компонентів $K = \{K_{i1},...,K_{iY}\}$, що реалізує миожину функцій $F = \{F_{i1},...,F_{iZ}\}$. Крім того для кожної і множин K_i і F_i в процесі еволюції можуть бути виділини дві наступні підмножини:

- підмножина компонентів, що змінюється $\Delta K = \{K_{i1},...,K_{iY1}\}$ і функцій що змінюються

$\Delta F = \{F_{i1},...,F_{iY1}\}$;

- підмножина компонентів, що не змінюється $\delta K = \{K_{i1},...,K_{iY2}\}$ і функцій, що не змінюється $\delta F = \{F_{i1},...,F_{iY2}\}$. При цьому $\Delta K_i \cup \delta K_i = K_i$; $\Delta K_i \cap \delta K_i = \varnothing$; $\Delta F_i \cup \delta F_i = F_i$; $\Delta F_i \cap \delta F_i = \varnothing$.

Висновки. Таким чином, на основі аналізу тенденцій розвитку систем пожежної сигналізації, а також останніх досягнень радіоелектроніки й інформаційної техніки можна сформулювати основні вимоги, яким повинна задовольняти сучасна автоматизована система керування оперативним пожежегасінням. Переведення існуючих систем пожежної сигналізації на нову структуру вимагає часу й значних матеріальних витрат, оскільки відсутня приємственість між існуючими системами пожежної сигналізації, що вже експлуатуються, і новими. Щоб повною мірою використати створену на основі засобів обчислювальної й мікропроцесорної техніки систему пожежегасіння, необхідно для кожного інформаційного фактора пожежі (дим, тепло, випромінювання полум'я й т.п.), а також для їхніх певних комбінацій розробити математичні моделі й відповідне інформаційне забезпечення на основі досить великого й експериментального матеріалу, що містить статистичну повноту.

Література

1. Якименко О., Скоробагатько Т. Стан із пожежами та наслідками від них в першому півріччі 2006 року // Пожежна безпека. – 2006. – № 8. – С. 30-31.

2. Тимченко А.А., Підгорний М.В., Однороманенко С.Г. Системне проектування автоматизованих систем керування оперативним пожежегасінням // Радіоелектронні і комп'ютерні системи. – 2006. – № 5. – С. 91-96.

3. Бюлетень пожежної безпеки (науково-технічні проблеми та рішення) // Пожежна безпека. – 2002. – № 6. – С. 14-16.

4. Підгорний М.В., Мельник В.П. Підвищення якості проектних рішень в системах забезпечення пожежної безпеки об'єктів // Тези доповідей V Ш-Міжнар. конф. «Контроль і управління в складних системах» (КУСС-2005). – Вінниця: УНІВЕРСУМ-Вінниця. – 2005. – С.200.

5. Патент України № 51574С2, МПК G08B25/08. Спосіб оповіщення про стан об'єктових кінцевих пристроїв; Публ. Бюл. «Промислова власність» № 3 15.03.05

Надійшла 22.2.2007 р.

УДК 004.31, 004.056.55, 003.26

М. П. КАРПІНСЬКИЙ
Університет в Бельску-Бялей, Польща
Л.М. КОРКІШКО
Тернопільський національний економічний університет
Т.А. КОРКІШКО
Інститут передових технологій Самсунг Електронікс, Південна Корея

АДАПТУВАННЯ АЛГОРИТМІВ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ (АКП) ДО ОБРОБКИ МАСКОВАНИХ ДАНИХ

Наведено методику адаптування АКП до обробки маскованих даних на основі заміни базових операцій цих алгоритмів на відповідні еквіваленти. У порівнянні із процесом розробки нових АКП, запропонована методика не вимагає всебічного математичного аналізу стійкості нових алгоритмів, добре інтегрується у процес проектування обчислювальних засобів для виконання АКП та дозволяє отримати адаптовані АКП із заданим рівнем безпекипроцесу їх виконання на цільовій комп'ютерній платформі.

Вступ

АКП часто реалізують на основі комп'ютерних платформ (апаратно чи програмно). Традиційно такі АКП реалізуються згідно з їх описом, поданим, як правило, у вигляді стандарту чи іншої специфікації. Разом з тим, широке розповсюдження мобільних комп'ютерних платформ та виконання АКП на цих платформах створюють загрози витоку конфіденційної інформації (ключі шифрування), яка використовується при обробці даних згідно з цими алгоритмами. Одним із основних способів реалізації цих загроз є проведення так званих інженерно-криптографічних атак з використанням інформації з побічних каналів витоку [1]. Такі канали витоку інформації часто створюються внаслідок існування залежності деяких характеристик платформи (споживана потужність, час обчислень, електромагнітне випромінювання тощо.) від конфіденційних даних, які обробляються. З метою уникнення (мінімізування) витоку корисної для атакуючого інформації у побічні канали застосовують масковане представлення інформації (даних і ключів) на основі техніки розділення таємниці [2]. Реалізація маскованого представлення інформації можна проводити як на технологічному рівні (на базі спеціалізованих логічних елементів) [3], так і на алгоритмічному рівні шляхом адаптування заданих АКП до