интеллектуального измерительного робота может быть использована для принятия решения и построения планов действий интеллектуальным измерительным роботом, функционирующим при нечеткой исходной информации, характеризующей реальное производство.

Литература

1. Egerstedt M., Hu X., Stotsky A. Control of a Car-Like Robot Using a Dynamic Model. Proc. of the IEEE Inter. Confer. on Robotics and Automation, Lenven, Belgium, v.4, pp.3273-3278, 1998.

2. Sordalen O. J., Canudas de Wit C. Exponential Control Low for a Mobile Robot: Extension to Path Following. IEEE Trans. On Rob. And Autom., Vol.9, No 6, pp.837-842, 1993.

3. Пат. РФ № 2185279. Пшихопов В.Х. Устройство позиционно-траекторного управления мобильным роботом, бюл. № 20, 2002.

4. Пшихопов В.Х. Аналитический синтез синергетических регуляторов для позиционно-траекторных систем управления мобильными роботами / В.Х. Пшихопов. – Сборник трудов научно-технической конференции «Экстремальная робототехника». – Под научной ред. проф. Юревича Е.И. – Центральный научно-сследовательский институт робототехники и технической кибернетики. – Санкт-Петербург, 2001. – С.59-68.

5. Люггер, Джорж Ф. Искусственный интеллект: стратегии и методы решения сложных проблем / Люггер, Джорж Ф., 4-е издание.: Пер. с англ. -М.: Издательский дом "Вильямс", 2003. -864с.

6. Алиев Р. А. Управления производством при нечеткой исходной информации / Р. А. Алиев, А. Э. Церковный, Г. А. Мамедова. – М.: Энергоатомиздат, 1991.– 240 с.

Надійшла до редакції
19.2.2013 р.

УДК 004

І.В. МУЛЯР, А.В. ДЖУЛІЙ, М.В. КОСТЮК
Хмельницький національний університет

АНАЛІЗ ПРОБЛЕМ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБРОБКИ ДАНИХ

Досліджено проблеми забезпечення функціональної безпеки інформаційних систем обробки даних, які використовують програмні засоби, що визначають *принципову можливість і ефективність їх застосування.. Вимоги до функціональної безпеки системи виникають з цілей забезпечення безпеки об'єктів та їх компонентів, що реалізують призначення та основні функції системи.*

Ключові слова: функціональна безпека, загрози, вразливості, рівні функціональної безпеки

The problems of security of information systems functional data, using software tools that define the fundamental feasibility and effectiveness of their application.. Requirements for the functional safety of the system arising from the purposes of security objects and their components that implement the purpose and main features of the system.

Keywords: functional safety, threat, vulnerability, levels of functional safety

Вступ

Інформаційна система, як система управління, тісно пов'язується, як з системами збереження та видачі інформації, так і з системами, що забезпечують обмін інформацією в процесі управління. Вона охоплює сукупність засобів та методів, що дозволяють користувачу збирати, зберігати, передавати і обробляти відібрану інформацію. Інформаційні системи існують з моменту появи суспільства, оскільки на кожній стадії його розвитку існує потреба в управлінні. Місією інформаційної системи є виробництво потрібної для організації інформації, потрібної для ефективного управління всіма її ресурсами, створення інформаційного та технічного середовища для управління її діяльністю. Інформаційні системи управління вирішуються задачі трьох типів:

- задачі оцінки ситуації (деколи їх називають задачами розпізнавання образів);
- задачі перетворення опису ситуації (розрахункові задачі, задачі моделювання);
- задачі прийняття рішень (в тому числі і оптимізаційні).

Автоматизована інформаційна система – це взаємозв'язана сукупність даних, обладнання, програмних засобів, персоналу, стандартних процедур, які призначені для збору, обробки, розподілу, зберігання, представлення інформації у відповідності з вимогами, які випливають з цілей організації.

Інформаційні системи включають в себе: технічні засоби обробки даних, програмне забезпечення і відповідний персонал. Основними факторами, які впливають на впровадження інформаційних систем, є потреби організацій та користувачів, а також наявність відповідних засобів для їх формування. Найсуттєвіше на розвиток інформаційних систем вплинули досягнення в галузі комп'ютерної техніки та телекомунікаційних мереж. Причини, що спонукають організації впроваджувати інформаційні системи, з одного боку обумовлюються прагненням збільшити продуктивність повсякденних робіт чи усунути їх

повторне проведення, а з іншого боку бажанням підвищити ефективність управління діяльністю організації за рахунок прийняття оптимальних та раціональних управлінських рішень.

Поставка задачі

Інформаційна система – комплекс, що включає обчислювальне і комунікаційне устаткування, програмне забезпечення, лінгвістичні засоби і інформаційні ресурси, використовує сучасні інформаційні і комп'ютерні технології, забезпечує організаційну, управлінську і виробничу діяльність компанії. Структура інформаційної системи подана на рис. 1. Однією із складових інформаційної системи (ІС) є система захисту інформаційної системи (СЗІС). СЗІС – підмножина функцій інформаційної системи, які відносяться до забезпечення захисту інформації.

Система захисту інформаційної системи повинна забезпечувати: захист центру управління, інформаційних ресурсів і засобів абонентського рівня від несанкціонованого доступу, у тому числі розмежування повноважень користувачів при доступі до ресурсів; забезпечення захисту програмних продуктів, засобів обчислювальної техніки від вторгнення "вірусів" і закладок; забезпечення необхідного рівня захисту від атак нелегальних користувачів до інформаційних ресурсів, що захищаються; захист інформації криптографічними методами з урахуванням рівня конфіденційності; системну підтримку і сервісне обслуговування засобів захисту інформації, підтвердження автентичності об'єктів даних і користувачів, виявлення порушень цілісності об'єктів даних, забезпечення захисту технічних засобів.

У системах, в яких результати обробки інформації та керуючі впливи безпосередньо визначають працездатність і якість функціонування складних систем управління в надзвичайних ситуаціях, не виключені аварії і катастрофи внаслідок недостатньої безпеки інформаційних систем. У вимогах технічних завдань і реалізованих проектах складних систем, пов'язаних з безпекою, систематично замовчуються і/або недостатньо формалізуються поняття і метрики безпеки інформаційної системи і інформації, що видається, якими характеристиками вони повинні описуватися, як їх слід вимірювати і порівнювати з вимогами, відображеними в контракті, технічному завданні або специфікації. Крім того, деякі з характеристик функціональної безпеки часто взагалі відсутні у вимогах замовника і погоджених документах на інформаційну систему, що призводить до довільного їх обліку або до пропуску при випробуваннях. Цьому сприяє обмеженість ресурсів, необхідних для досягнення і оцінювання у процесах життєвого циклу систем, необхідних і реалізованих значень безпеки, а також недостатня формалізація і документування всього процесу їх вибору та аналізу.

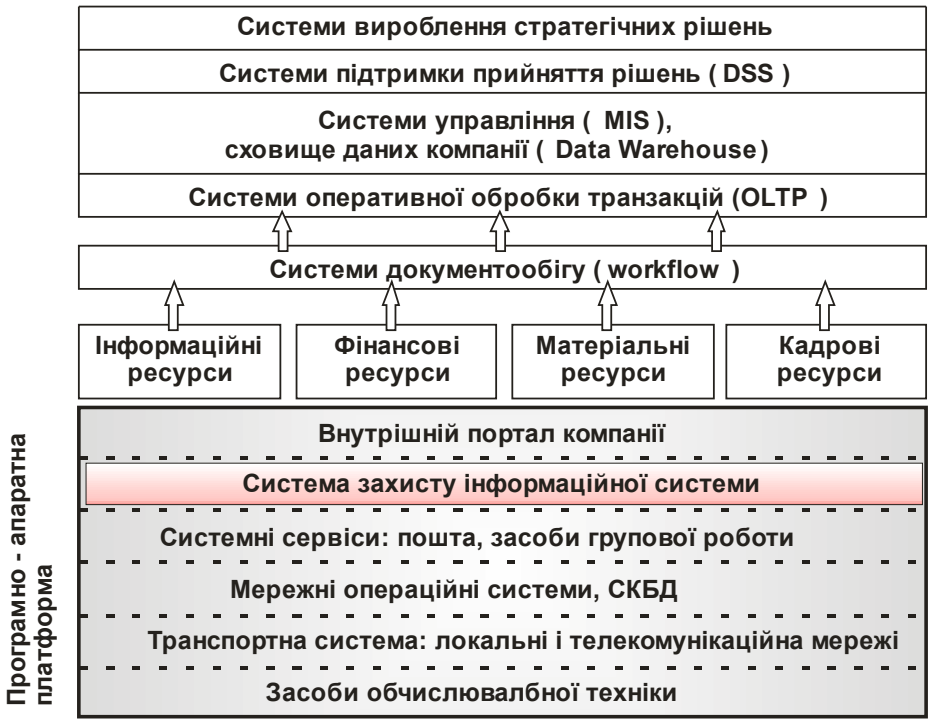

Рис. 1. Структура інформаційної системи

Основна частина

В умовах використання ІС під безпекою розуміється стан захищеності ІС від внутрішніх і зовнішніх загроз. Показник захищеності ІС – характеристика засобів системи, що впливає на захищеність, яка визначена певною групою вимог, варійованих за рівнем і глибиною залежно від класу захищеності. Безпечна система забезпечує управління доступом до інформації, таким чином, що тільки авторизовані особи або процеси, що діють від їхнього імені, отримують право працювати з інформацією. Надійна система – система, що використовує апаратні і програмні засоби для забезпечення одночасної обробки інформації

різної категорії секретності групою користувачів без порушення прав доступу. Політика безпеки – набір законів, правил і практичного досвіду, на основі яких будується керування, захист і розподіл конфіденційної інформації.

Для оцінки реального стану функціональної безпеки ІС можуть застосовуватися різні критерії. Аналіз вітчизняного та зарубіжного досвіду показав певну спільність підходу до визначення стану функціональної безпеки ІС в різних країнах. Для надання користувачеві можливості оцінки вводиться деяка система показників і задається ієрархія класів безпеки. Кожному класу відповідає певна сукупність обов'язкових функцій. Ступінь реалізації обраних критеріїв показує поточний стан функціональної безпеки. Подальші дії зводяться до порівняння реальних загроз із реальним станом функціональної безпеки. Якщо реальний стан перекриває загрози в повній мірі, система безпеки вважається надійною і не вимагає додаткових заходів. Таку систему можна віднести до класу з повним перекриттям загроз і каналів витоку інформації. В іншому випадку система безпеки потребує додаткових заходів захисту.

Національний центр комп'ютерної безпеки міністерства оборони США (National Computer Security Center) розробив критерії оцінки рівня функціональної безпеки інформаційної системи. Ця класифікація на сьогоднішній день є загальновизнаною і вона стала загальноприйнятим світовим стандартом.

Цей документ містить основні вимоги та специфікує класи для оцінки рівня функціональної безпеки інформаційної системи. Можливості аналізу рівня функціональної безпеки ІС призвели до міжнародного визнання федерального стандарту США.

У цьому документі наводяться такі рівні функціональної безпеки інформаційної системи:

- А – високий рівень;
- В – проміжний рівень;
- С – низький рівень безпеки;
- Д – клас систем, що не пройшли випробування.

Рівень А забезпечує гарантований рівень безпеки. Методи захисту, реалізовані в системі, можуть бути перевірені формальними методами. Рівень В представляє повний захист ІС. У цій групі виділено класи безпеки В1, В2 і В3. У системах класу В, що містить три підкласи повинен бути повністю контрольований доступ. Повинні виконуватися ряд вимог, головною з яких є наявність добре визначеної і документованої формальної моделі політики безпеки, що вимагає дії виборчого і повноважного управління інформаційними потоками відповідно до політики безпеки. Класи В1 – В3 відрізняються ступенем допустимого доступу до частин системи, підсистем і блокам інформації, а також контролем доступу до них користувачів. Рівень С представляє виборчий захист підсистем з контролем доступу до них користувачів. У цій групі виділено класи безпеки С1 і С2. Клас С1 передбачає поділ в ІС користувачів і даних. Цей клас забезпечує найнижчий рівень захисту ІС. Клас С2 – забезпечується роздільним доступом користувачів до даних. Рівень Д – складають ІС перевірені на безпеку, але які не можуть бути віднесені до класів А, В або С.

Приведені рівні дозволяють оцінити реальну функціональну безпеку інформаційної системи з віднесенням її до певного рівня захищеності. Рівень захищеності ІС – певна сукупність вимог щодо захисту ресурсів ІС від несанкціонованого доступу до інформації. Політика безпеки ІС повинна будуватися з урахуванням перерахованих вище нормативних матеріалів. Слід пам'ятати, що в політиці безпеки ІС немає дрібниць, тому що жодна з систем не є абсолютно безпечною.

Безперервно зростаюча складність і внаслідок цього вразливість інформаційних систем від випадкових і навмисних негативних впливів висунули ряд проблем, пов'язаних з безпекою систем, які використовують програмні засоби, в розряд найважливіших – стратегічних, що визначають принципову можливість і ефективність їх застосування. При цьому виділилися області аналізу і забезпечення інформаційної безпеки, пов'язані, в основному, із захистом від навмисних, негативних впливів на інформаційні ресурси систем і функціональної безпеки.

Проблема забезпечення інформаційної безпеки функціонування ІС у процесі розробки та експлуатації виникла і розвивається внаслідок зростання складності та відповідальності завдань використання інформаційних ресурсів і збільшення їх вразливості від атак нелегальних користувачів, з метою незаконного використання або спотворення інформації та програм, які за своїм змістом призначені для застосування обмеженим колом осіб. Основна увага в сучасній теорії та практиці забезпечення функціональної безпеки інформаційних систем зосереджена на захисті від злочинних руйнувань, перекручувань, розкрадань та використання програмних засобів та інформації баз даних. Для цього розроблені та активно розвиваються проблемно-орієнтовані методи та засоби захисту від несанкціонованого доступу, від різних типів «вірусів» і закладок, від просочування інформації по каналах електромагнітного випромінювання і т. ін. Ретельна специфікація і оцінювання функціональної безпеки систем, програмного продукту і обробленої для користувачів інформації – ключовий фактор забезпечення їх ефективного і адекватного застосування. Це може бути досягнуто на основі виділення, визначення та забезпечення відповідних характеристик з урахуванням цілей використання і функціональних завдань інформаційних систем.

У процесі проектування, розробки і всього життєвого циклу основних функціональних завдань, операційного середовища, апаратури ЕОМ ці компоненти з часом розвиваються й адаптуються, що відображається на необхідності адекватної зміни методів, завдань та засобів забезпечення їх функціональної безпеки. Таким чином, проблеми забезпечення функціональної безпеки складних систем повинні

вирішуватися з урахуванням одночасного динамічного розвитку всіх компонентів середовища і факторів, які безперервно змінюються і впливають на результати їх вирішення. Однак такий складний, безперервний, багатозв'язковий процес важко реалізувати практично і його доцільно вирішувати поетапно, можливо з необхідними ітераціями і спрощеннями. При цьому слід мати на увазі, що завжди можуть проявитися віддалені зв'язки процесів, які можуть істотно вплинути на поточні роботи з забезпечення безпеки системи.

У процесі системного аналізу та проектування повинні бути виявлені потенційні навмисні і випадкові загрози функціонуванню ІС і встановлений необхідний рівень безпеки цього комплексу програм. У відповідності з цим рівнем замовником та розробниками повинні вибиратися і встановлюватися необхідні набори методів, властивостей і засобів забезпечення безпеки ІС з врахуванням обмежених ресурсів на їх реалізацію. У результаті сформовані вимоги повинні забезпечувати достатній захист від різних реальних загроз і реалізацію необхідних заходів контролю і підтвердження необхідних характеристик функціональної придатності комплексу програм в умовах загроз безпеці функціонування ІС. Для забезпечення ефективності системи, комплекс програм, пов'язаний з безпекою, доцільно базувати на наступних загальних принципах:

- захист апаратури системи, функціональних програм і даних повинен бути комплексним і багаторівневим, орієнтованим на всі види загроз з урахуванням їхньої небезпеки для користувача;
- вартість (трудомісткість) створення та експлуатації системи програмного захисту повинна бути менше, ніж розміри найбільш вірогідного або можливого (в середньому) неприйнятного користувачами системи збитку – ризику від будь-яких потенційних загроз;
- набір функцій захисту повинен мати цільові, індивідуальні компоненти контрзаходів, призначені для забезпечення безпеки функціонування кожного окремо взятого компонента та функціональної задачі системи з урахуванням їх вразливості і ступеня впливу на безпеку системи в цілому;
- система захисту інформаційної системи не повинна призводити до відчутних труднощів, перешкод і зниження ефективності застосування і вирішення основних, функціональних завдань користувачами системи в цілому.

Характеристики зовнішнього середовища, прикладні сфери застосування комплексів програм, цілі і завдання користувачів, рівень автоматизації їх функцій і багато інших чинників визначають методи і властивості засобів забезпечення безпеки обчислювальних систем.

В основу формування вимог до функціональної безпеки має бути покладено визначення переліку та характеристик потенційних загроз безпеки і встановлення можливих джерел їх виникнення. Дестабілізуючими чинниками, що створюють загрози безпеці функціонування інформаційної системи є:

- навмисні, негативні впливи осіб з метою спотворення, знищення або розкрадання програм, даних і документів інформаційної системи, як наслідки порушення інформаційної безпеки, що відображаються також на функціональній безпеці;
- помилки і несанкціоновані дії оперативного, адміністративного та обслуговуючого персоналу в процесі експлуатації інформаційної системи;
- спотворення в каналах телекомунікації інформації, що надходить від зовнішніх джерел і переданої користувачам, а також неприпустимі значення та зміни характеристик потоків інформації від об'єктів зовнішнього середовища;
- збої і відмови в апаратурі обчислювальних засобів;
- віруси, збої і відмови, поширювані каналами телекомунікації, що впливають на інформаційну та функціональну безпеку ІС;
- зміни складу і конфігурації комплексу взаємодіючої апаратури системи за межі, перевірені при випробуваннях або сертифікації.

Повне усунення перерахованих вище загроз безпеки функціонування системи принципово неможливо. При створенні складних комплексів програм проблема полягає в виявленні факторів, від яких вони залежать, у створенні методів і засобів зменшення їх впливу на безпеку. Необхідно оцінювати вразливість функціональних компонентів системи для різних негативних впливів і ступінь їх впливу на основні характеристики якості та безпеки системи, а також на сумарний ризик, що визначає рівень функціональної безпеки інформаційної системи. Залежно від цього слід розподіляти ресурси для створення системи та її компонентів, рівнозначних з безпеки функціонування з мінімальним ризиком узагальненим за будь-яких негативних зовнішніх впливах. У результаті мають бути сформульовані відповідні методи та контрзаходи, які, в свою чергу, визначають необхідні функції і механізми засобів забезпечення працездатності та безпеки системи.

Стандартами рекомендується, щоб було передбачено вимірювання або оцінювання кожної характеристики ІС з точністю і визначеністю, достатньою для порівнянь з вимогами технічних завдань та специфікацій, і щоб вимірювання були об'єктивні і відтворювані. Слід передбачати норми допустимих помилок вимірювання, викликаних інструментами та / або помилками людини-експерта. Щоб вимірювання були об'єктивними, повинна бути документально підтверджена, узгоджена процедура для присвоєння числового значення, властивості або категорії кожному атрибуту програмного продукту. Процедури вимірювань повинні давати в результаті однакові заходи з прийнятною стійкістю, одержаними різними суб'єктами при виконанні одних і тих же оцінок характеристик ІС. Характеристики якості ІС з позиції можливості і точності їх вимірювання можна розділити на три рівні деталізації показників, особливості яких слід уточнювати при їх виборі:

- категорійні-описові, що відображають набір властивостей і загальні характеристики об'єкта – його функції, категорії відповідальності, безпеки та важливості, які можуть бути представлені номінальною шкалою-категорій властивостей;
- кількісні – подаються множиною упорядкованих числових точок, що відбивають безперервні або дискретні закономірності й описувані інтервальною або відносною шкалою, які можна об'єктивно виміряти та чисельно зіставити з вимогами;
- якісні – містять кілька впорядкованих або окремих властивостей- категорій, які характеризуються порядковою або точкової шкалою набору категорій (є – немає, добре – погано), встановлюються, вибираються й оцінюються в значній мірі суб'єктивно та експертно.

До першого рівня відносяться показники якості, які характеризуються найбільшою різноманітністю значень – властивостей програм і наборів даних і охоплюють весь спектр класів, призначень і функцій сучасних ІС. Ці властивості можна порівнювати тільки в межах однотипних ІС і важко впорядковувати за принципом переваги. Серед стандартизованих показників якості до цієї групи, перш за все, відноситься функціональна безпека, яка є найважливішою і домінуючою характеристикою будь-яких ІС. Номенклатура і значення всіх інших показників якості безпосередньо визначаються необхідними функціями програмного засобу і, в тій чи іншій мірі, впливають на виконання цих функцій.

До другого рівня показників якості відносяться досить достовірно і об'єктивно вимірювані чисельні характеристики ІС. Значення цих конструктивних характеристик зазвичай найбільшою мірою впливають на функціональну безпеку і метрики у використанні ІС. Тому вибір та обгрунтування їх необхідних значень повинні проводитися найбільш вірогідно вже при проектуванні ІС. Їх значення можуть бути описані впорядкованими шкалами об'єктивно вимірюваних значень, необхідні чисельні величини яких можуть бути встановлені і обрані замовниками або користувачами ІС.

Третій рівень стандартизованих показників якості ІС важко повністю описати вимірюваними кількісними значеннями і їх значення мають описовий, якісний вигляд. Залежно від функціонального призначення ІС за погодженням із замовником можна визначати експертно ступінь необхідності (пріоритет) цих властивостей і бальні значення рівня реалізації їх атрибутів у життєвому циклі конкретної ІС.

При подальшому аналізі увага акцентується на визначенні вимог і застосуванні складних апаратно-програмних систем і на їх функціональній безпеці. Відповідно збиток при відмовних ситуаціях визначається вразливістю і порушенням коректного виконання системою основного призначення і необхідних функцій при обмежених ресурсах на їх реалізацію. Вимоги до функціональної безпеки системи виникають з цілей забезпечення безпеки об'єктів та їх компонентів, що реалізують призначення та основні функції системи, а також з цілей забезпечення безпеки її середовища. Такий поділ грунтується на сукупному обліку інженерного досвіду, політики безпеки, економічних факторів і аналізу ризиків.

Висновок

Вимоги безпеки є результатом перетворення загальних цілей безпеки системи в сукупність вимог безпеки для функціональних об'єктів та вимог безпеки для зовнішнього середовища, які, в разі їх задоволення, повинні забезпечити для системи здатність досягнення її базових цілей функціональної безпеки. Середовище забезпечення функціональної безпеки ІС включає політики та програми організації безпеки підприємств і систем, досвід, спеціальні навички і знання, що визначають контекст передбачуваного застосування системи. Середовище включає також можливі загрози безпеки, присутність яких у цьому середовищі встановлено або передбачаються. При формалізації середовища функціональної безпеки слід брати до уваги:

- призначення інформаційної системи, включаючи функції програмного забезпечення і передбачувану сферу його застосування;
- активи – програми і дані функціональних завдань системи, які вимагають забезпечення безпеки, до яких застосовуються вимоги та / або політики безпеки, а також компоненти, які підпорядковані вимогам безпеки інформаційної системи;
- фізичне середовище в тій її частині, яка визначає всі аспекти експлуатаційного середовища системи, що стосуються безпеки, включаючи заходи, пов'язані з засобами фізичного захисту і персоналу.

На підставі розроблених політик безпеки, оцінок загроз і ризиків слід сформувати вхідні дані, пов'язані з функціональною безпекою середовища системи і основного комплексу програм:

- припущення, яким повинне задовольняти середовище для того, щоб інформаційна система вважалася безпечною;
- загрози безпеці для активів, в яких були б ідентифіковані всі загрози середовища, прогнозовані на основі аналізу безпеки, які відносяться до об'єкта функціональної безпеки;
- загрози, які розкриваються через поняття джерела загроз, передбачуваного методу їх реалізації, передумови для відмов та ідентифікація компонентів, які є об'єктами відмов;
- політика безпеки, в якій були б достатньо точно ідентифіковані та описані цілі, методи і правила реалізації функціональної безпеки системи.

Література

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. / В.А. Герасименко – В 2-х кн. – М.: Энергоатомиздат, 1994.

2. Баранов А.П. Математические основы информационной безопасности / А.П. Баранов, Н.П. Борисенко, А.Г. Ростовцев. – Орел : ВИПС, 1997. – 354 с.

3. Джулій А.В. Імовірнісна модель програмно-апаратного захисту інформаційної системи / А.В. Джулій, В.М. Джулій // Вісник Хмельницького національного університету. – 2008. – № 4. – С. 70-75.

4. Джулій А.В. Оцінка адекватності математичної моделі процесу функціонування системи захисту // IV міжнародна науково-практична конференція «Інтегровані інтелектуальні робото-технічні комплекси». НАУ. – К : , 2011. – С. 402-404.

5. Домарев В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев. – К.: ООО «ТИД ДС», 2004. – 992 с.

Надійшла до редакції
06.3.2013 р.

УДК 004.08.01

З.І. ДОМБРОВСЬКИЙ, А.М. БОРОВИЙ, В.В. КОЧАН
Тернопільський національний економічний університет

КОМП'ЮТЕРНА ІНФОРМАЦІЙНА СИСТЕМА ДЛЯ ОЦІНКИ СТРУМУ СПОЖИВАННЯ МІКРОПРОЦЕСОРІВ ПРИ ВИКОНАННІ ІНСТРУКЦІЙ

Розглянуто побудову комп'ютерної інформаційної системи для оцінки та прогнозування струму споживання мікропроцесорів при виконанні інструкцій.

Ключові слова: комп'ютерна система, оцінка, прогнозування, струм споживання мікропроцесора.

It is considered the construction of computer information system for assessing and forecasting power consumption of microprocessors during the instructions execution.

Keywords: computer system score, prediction, current consumption of the microprocessor.

Вступ. За прогнозами Intel до 2015 р. кількість комп'ютерних систем (КС) з автономним живленням перевищить 15 млрд. Для живлення автономних систем використовують енергетично обмежені ресурси (акумулятори), тому тривалість роботи є важливим фактором їх використання в автономному режимі [1]. Отже пошук методів збільшення тривалості роботи комп'ютерних систем при автономному живленні є важливою частиною використання таких систем.

Постановка задачі. Дослідження в області збільшення тривалості роботи КІС при автономному живленні проводять за трьома напрямками:

1) удосконалення джерел живлення;

2) зменшення споживання апаратних засобів;

3) оптимізація споживання програмної складової.

На сьогодні переважають заходи зменшення енергоспоживання, за рахунок удосконалення джерел живлення та оптимізації апаратної складової КС. Задачу мінімізації енергоспоживання на етапі проектування КС [7] розв'язують використовуючи стандартизовані методи проектування, що дозволяє зменшити видатки на проектування як системи загалом, так і окремих компонентів, з врахуванням їх енергоспоживання [5].

В результаті зменшення затрат на проектування комп'ютерних систем, з врахуванням не лише специфікацій, але й мінімізації використання ресурсів (а отже й енергоспоживання) може сягати 20 % [8, 9].

Проведений аналіз [2,3], вказує на те, що для автономних систем процесор є одним з енергоємних пристроїв, а тому оптимізація його енергоспоживання (і як наслідок збільшення тривалості роботи системи на одному заряді) є першочерговою. Для мінімізації споживання енергії та забезпечення максимального терміну роботи при живленні від автономних джерел без обмежень [2] щодо виконання інформаційних задач застосовують такі методи [3]: впровадження нових архітектурних та технологічних рішень на етапі проектування системи; оптимізація програмного забезпечення нових та існуючих систем.

В той час, як велика кількість виробників зосереджується на апаратній оптимізації енергоспоживання кінцевого пристрою, програмна складова в основному залишається поза увагою, хоча її вплив на кінцеве енергоспоживання процесора є незаперечним. Таке спрощення мотивується тим, що процес оцінки енергоспоживання ПЗ є складною, комплексною проблемою, і потребує розв'язання декількох задач. Отже актуальним є потреба нових підходів щодо зменшення потужності при виконанні інструкцій мікропроцесора в комп'ютерних системах з автономним живленням.

Для досягнення мети необхідно запропонувати концепцію функціонування комп'ютерної системи та розробити відповідне ПЗ.

Основна частина. Вперше дослідження залежності споживання при виконанні інструкцій проводив