УДК 004.4.242

О.В. Бойченко[1], О.С. Лєнков[2]

[1]*Національний авіаційний університет, Київ*
[2]*Військовий інститут Київського національного університету ім. Т. Шевченка, Київ*

МЕТОДИКА УПРАВЛІННЯ ЗАХИСТОМ ДАНИХ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА ОСНОВІ МЕТОДУ ПАРОЛІВ ТА ТЕСТОВИХ ІНТЕРФЕЙСІВ

Розглядається питання проблематики управління захистом даних інформаційних систем реального часу. Запропонована методика управління захистом інформаційної системи на основі методу паролів та тестових інтерфейсів, що дозволяє забезпечити стійкість на рівні макроструктури організуючої системи.

Ключові слова: *інформаційна система, система захисту, пароль, тестовий інтерфейс.*

Вступ

Постановка проблеми. З розвитком науково-технічного прогресу забезпечується все більше зростання застосування комп'ютерних технологій в усіх напрямах життєдіяльності суспільства. Поряд із зазначеним все більш нагальною стає потреба в захисті даних, які циркулюють у складі інформаційно-телекомунікаційних систем, від несанкціонованого доступу. Це визначено зростанням кількості злочинів у сфері інтелектуальної власності та інформаційних технологій. Зростання науково-технічного прогресу обумовлює негативні тенденції розвитку злочинного світу, приводить до появи нових форм і видів злочинних посягань за рахунок того, що злочинні групи активно використовують у своїй діяльності новітні досягнення науки і техніки, застосовують сучасні інформаційно-телекомунікаційні технології [1].

Мета роботи полягає у розробці методики виявлення несанкціонованого впливу на програмне забезпечення в системі управління захистом даних інформаційної системи на основі методу паролів та тестових інтерфейсів.

Виклад основного матеріалу

Для вирішення поставленого завдання найбільш доцільно застосовувати комплексний спосіб захисту електронних інформаційних системна основі багато режимного характеру інформаційних сервісів шляхом встановлення необхідної комбінації авторизації, зворотного зв'язку й криптографічних способів захисту цілісності інформаційного середовища з врахуванням багато вимірності послідовності дій клієнта системи [2]. Однак, незважаючи на обладнання таким захистом усіх шарів структури, послідовність виконання може бути порушена входженням програми в безкінечний цикл, виконанням циклу невірною кількістю раз або виконанням виходу через недійсну гілку.

Розглянемо застосування вбудованого контролю для виявлення й діагностування помилки, пов'язаної с порушенням правильності послідовності виконання елементів ПЗ [3]. Послідовність виконання може бути порушена одним з таких способів:

програма входить у безкінечний цикл;

цикл виконується невірне число разів;

виконується вихід через неіснуючу гілку (гілку, якої нема у ПЗ);

при переході вибрана неправільна гілка.

Перевірка виходів на неіснуючу гілку реалізується установленням пароля (П: = 1) при вході у структурний елемент S й перевіряється при виході з нього з наступним обнуленням (рис. 1, а). Не співпадіння пароля на виході структури свідчить про нелегальний вхід в неї (передачу управління повз вхідну точку) й призводить до ініціації діагностуючої задачі, яка перевіряє паролі всіх структур.

Оснащення таким захистом всіх шарів структури, починаючи з верхнього, дозволяє знайти в графі паролів, ізоморфному графу структури ПЗ (рис. 1, б), шлях від кореневої вершини, яка відмічена 1, до самого нижнього шару (кількість шарів залежить від необхідного ступеня деталізації при діагностиці й від припустимих втрат на надмірність, виявляючи елемент, в якому мав місце збій (чий пароль є необнуленим).

На рис. 2, а показаний захист паролями більш складної конструкції. Пароль П1 забезпечує виявлення нелегального входу в конструкцію IFP-THENS1-ELSES2 й діагностування з точністю до рівня цієї конструкції при нелегальному виході з неї. Паролі П2 й П3 дозволяють отримати діагностуємість на більш низькому рівні (захищені конструкції S1 й S2). Рис. 2, б подає фрагмент графа паролів для цього прикладу.

У структурі IFP-THENS1-ELSES2 можуть виникнути такі помилки: вибір помилкової гілки, тобто виконання гілки S1 замість S2; нелегальний вхід, тобто входження в конструкцію, оминаючи вхідну точку. Для контролю помилок в управлінні послідовністю розщеплюють вузол прийняття рішення на два послідовно з'єднаних вузла й додають надмірні блоки (рис. 2, а).

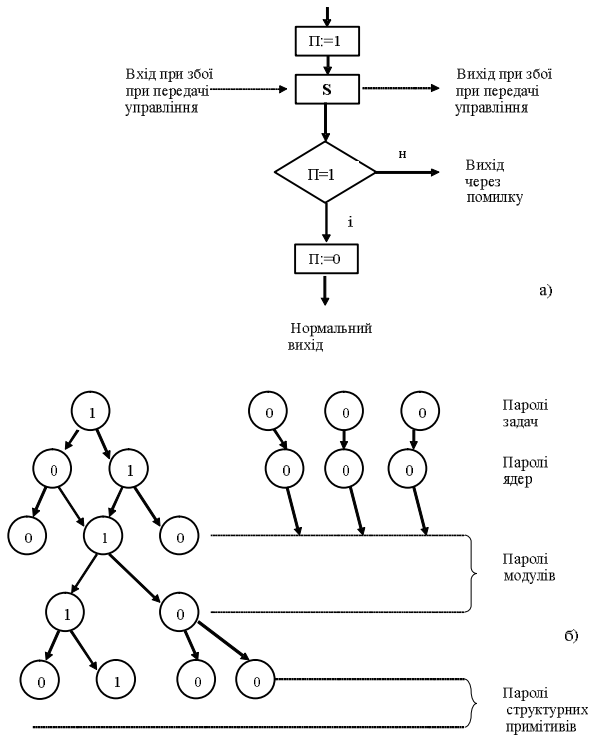

Рис. 1. Використання паролів для діагностування при збої при передачі управління

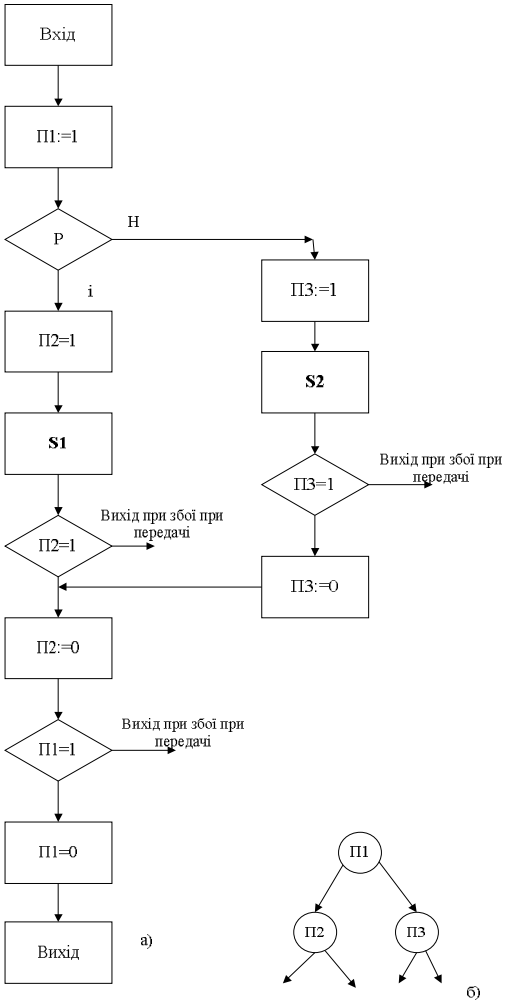

Рис. 2. Захист паролями структури IF P THEN S1 ELSE S2

Предікат $\overline{P}$ розуміється як заперечення предікату P, наприклад, якщо предікат P має вигляд

$$x > 0,$$

то предікат $\overline{P}$ приймає вигляд $x \le 0$.

Відповідно до методології пошарового структурного проектування, кожна проектована задача розбивається на два компоненти: функціональний (ядро) і той, що зв'язує ядра в систему через ОС (інтерфейс).

Ядро виконує продиктовані задачі функції й оформляється у вигляді підпрограми, керування якої передається з інтерфейсу.

За допомогою інтерфейсів між ядрами встановлюються зв'язки по керуванню (через операційну систему (ОС) і за даними (через базу даних, загальну частину або будь-який інший засіб). Інтерфейси, використовувані а процесі нормальної експлуатації, умовимося називати робочими інтерфейсами (РІ. РІ одержує керування від ОС і викликає на роботу ядро, передаючи йому необхідні дані. Після відпрацьовування ядра керування повертається на РІ. Результати розрахунку (вихідні дані ядра) передаються робочим інтерфейсом за призначенням. Керування через ОС передається наступній задачі (наступному РІ).

Структура задачі − ядро-інтерфейс − дозволяє організувати тестування ядра (у процесі проектування) методом тестового обрамлення. Суть методу полягає у використанні спеціального тестового інтерфейсу (ТІ). ТІ містить вхідні набори для перевірки маршрутів ядра і вихідні еталонні набори.

Передбачається використовувати тестові інтерфейси для контролю цілісності ядер у процесі нормальної експлуатації [4].

У ядро задачі закладаються засоби фіксації маршруту проходження опрацювання даних на реальному наборі даних (практично в кожну гілку програми ставиться лічильник, вектор лічильників доступний тестовому інтерфейсу). Ядро запускається на виконання через робочий інтерфейс.

Результати роботи тимчасово запам'ятовуються в робочому інтерфейсі. Тестовий інтерфейс за значенням вектора лічильників визначає гілку прогону і повторно запускає ядро з тестовим набором даних для цього маршруту [5] (рис. 3).

Дані відпрацювання порівнюються з еталонними. У випадку збігу («тест пройшов») із робочого інтерфейсу видаються результати першого прогону. У протилежному разі головна задача системи, що виконує функції підсистеми контролю, сповіщається про «несправність» ядра.

Результати першого прогону вважаються недійсними.

Нові наукові досягнення. Для організації контролю і відновлення користувачу повинні бути подані такі види послуг:

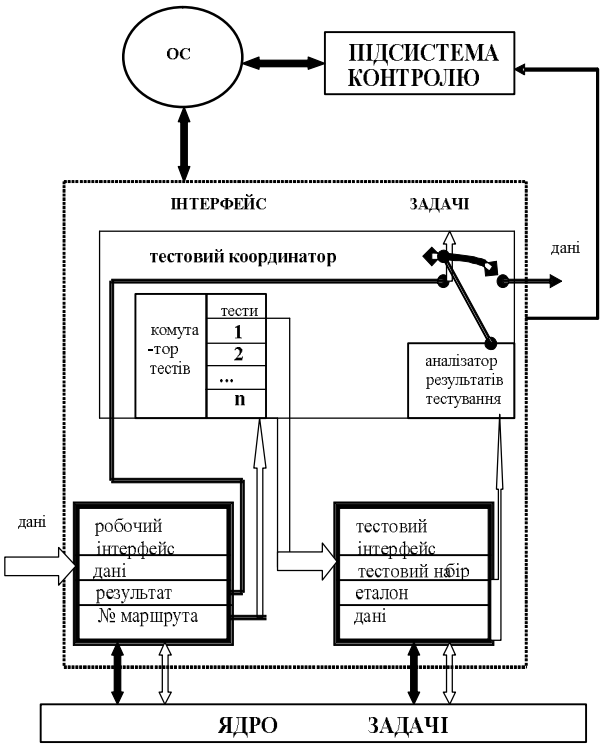

Рис. 3. Схема організації інтерфейсу задачі

розвинутий апарат контрольних точок;

коди завершення, що ідентифікують результати роботи при закінченні всіх операцій з ПВВ, НМД і псевдоустріями;

у багатопроцесорній ЕОМ при виході з ладу одного з процесорів повинний здійснюватися перехід на справний процесор без втручання (або при мінімальному втручанні) оператора;

примусове завершення виконання задач із програми користувача;

реалізація роздруківки діагностичних повідомлень для оператора з указівкою кодів завершення, слова стану процесора, імені задачі, при виконанні якої відбулося виявлення помилки;

дозвіл пересилки даних між розділами;

припущення резервування розділів ОЗП;

відкритість для нарощування додатковими модулями (агрегативність).

Висновки

Розроблена методика управління захистом даних інформаційної системи на основі методу паролів та тестових інтерфейсів дозволяє забезпечити стійкість на рівні макроструктури організуючої системи. Методика реалізується засобами, які дозволяють виявляти та оброблювати помилки та відмови пристроїв вводу-виводу при обміні; встановлювати перевищення допустимого часу реакції на запит процесора; виявляти звертання до захищених ділянок пам'яті (порушення адресації) та звертання до ресурсу, відсутнього в системі; встановлювати пошкодження ділянок оперативного запам'ятовуючого пристрою, зовнішньої пам'яті та перевантаження черги до ресурсу; виявляти помилки в виклику супервізора операційної системи в командах оператора, помилки переривання схем контролю процесора, помилки при читанні (запису) інформації з зовнішньої пам'яті та ін.

Список літератури

1. Бойченко О.В. Проблема кібертероризму у інформаційному забезпеченні підтримки рішень / О.В. Бойченко, Я.Я. Винярський, О.С. Лєнков // Інформаційна безпека. – Луганск, 2012. – № 2(8). – С. 9-14.

2. Пат. 68762 Україна, МПК (2012.01) G06K 9/00. Спосіб комплексного захисту інформації в автоматизованих системах спеціального призначення / О.В. Бойченко, З.З. Сітшаєва; заявник і власник О.В. Бойченко, З.З. Сітшаєва. – № и201111298; заявл. 23.09.2011; опубл. 10.04.2012, Бюл. № 7.

3. Турский В. Методология проектирования программ: моногр. / В. Турский. – М.: Мир, 1981. – 265 с.

4. Dijkstra E.W. Goto Statement considered harmful / Dijkstra E.W. // CACM 11. – 1968. – No 3. – Pp. 147-148.

5. Сбитнев А.И. Построение верификатора модульной системы на основе расширенных графов / А.И. Сбитнев // Кибернетика и вычислительная техника. – К., 1985. – С. 96-98.

Надійшла до редколегії 5.09.2012

Рецензент: д-р техн. наук, проф. І.В. Шостак, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

МЕТОДИКА УПРАВЛЕНИЯ ЗАЩИТОЙ ДАННЫХ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ МЕТОДА ПАРОЛЕЙ И ТЕСТОВЫХ ИНТЕРФЕЙСОВ

О.В. Бойченко, О.С. Ленков

Рассматривается вопрос проблематики управления защитой данных информационных систем реального времени. Предложена методика управления защитой информационной системы на основе метода паролей и тестовых интерфейсов, что позволяет обеспечить стойкость на уровне макроструктуры организующей системы.

Ключевые слова: *информационная система, система защиты, пароль, тестовый интерфейс.*

METHOD OF MANAGEMENT PROTECTION OF DATA OF INFORMATIVE SYSTEM ON BASIS OF METHOD OF PASSWORDS AND TEST INTERFACES

O.V. Boychenko, O.S. Lenkov

The question of problems of management defence of these informative real-time systems is examined. Offered method of management defence of the informative system on the basis of method of passwords and test interfaces, that allows to provide firmness at the level of macrostructure of the organizing system.

Keywords: *informative system, system of defence, password, test interface.*