Заключение

Из обобщения представленных данных следует, что разработанная модель РРВ дает хорошее совпадение с результатами эксперимента и может быть применена на практике для расчета защищенности радиолиний локальных ЦСПИ с широкополосными сигналами во всех трех зонах излучения как в случае закрытого помещения, так и вне его.

Предложенная модель названа авторами моделью ХНУРЭ Wi–Fi. Сравнивая кривые 1, 4, 5 на рис. 2, 3 нетрудно заключить, что модель ХНУРЭ Wi–Fi заметно выигрывает в точности получаемых результатов, по сравнению с известной моделью Хата COST 231. Этот выигрыш, на наш взгляд, обусловлен тем, что эмпирические зависимости РРВ были получены Окамура-Хата в 70-80г. XX века [4]. Тогда господствовала аналоговая связь и специфика ЦСПИ с широкополосными сигналами не нашла отражение в эмпирических соотношениях.

Таким образом, доказана гипотеза о возможности использования приближенной модели, основанной на отражательной трактовке, для расчета затуханий широкополосных сигналов в многолучевых радиолиниях локальных ЦСПИ с технологией Wi–Fi.

Работа выполнена при поддержке Государственного фонда фундаментальных исследований при Министерстве образования и науки Украины (Договор № Ф25/737-2007 от 03.09.2007 г.).

Список литературы

1. Бернард Скляр. Цифровая связь. Теоретические основы и практическое применение, 2-е издание: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 1104 с.

2. Никольский В.В. Электродинамика и распространение радиоволн. Учебное пособие. – М.: Изд-во «Наука», 1973. – 607 с.

3. EURO-COST 231TD (91)73. Urban transmission loss models for mobile radio in the 900 and 1800 MHz bands. – The Hague, September, 1991.

4. Hata M. Empirical formula for propagation loss in land mobile radio service / IEEE Trans. 1980. – VT-29, №3. – P. 317-325.

Поступила 27.02.2008г.

УДК 004.415.5

С.В.Лєнков, В.В. Балабін, О.М.Грищак

ГАРАНТУВАННЯ СТІЙКОСТІ ФУНКЦІОНУВАННЯ СПЕЦІАЛЬНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗА ДОПОМОГОЮ МЕТОДУ "ПАРОЛІВ"

Вступ та постановка завдання. Відомо, що стійкість функціонування найкращим чином гарантується вибором технології проектування, що оптимально використовує введення надмірності. Використання структурного проектування спеціального програмного забезпечення (надалі - СПЗ), що базується на використанні певних шарів і методології „згори-донизу", надає певних можливостей щодо забезпечення стійкості функціонування проектованого СПЗ.

Базою методології структурного проектування СПЗ є використання етапів, на кожному з яких розроблення ведеться пошарово на обмеженому наборі допустимих структур [1, 2]. Перший етап — етап проектування системних зв'язків (системна специфікація). Змістом цього етапу є тривимірна функціонально-подійно-режимна декомпозиція СПЗ на задачі. Другий етап —виділення функціонального ядра кожної задачі. Особливістю такого виділення є незалежність даної частини задачі від обраної операційної системи і обраного методу міжзадачного зв'язку за даними. Починаючи з даного етапу, розроблення ведеться за двома зустрічними напрямками: проектування ядер ведеться "згори донизу" (аналітичний підхід), остаточне збирання системи за допомогою інтерфейсів – "знизу вгору" (синтетичний підхід).

Третій етап полягає в пошаровому модульному проектуванні, який є подальшою декомпозицією функціональних ядер. На четвертому етапі виробляється деталізація модулів з використанням структурних примітивів структурного програмування.

Задача отримання коректного та стійкого до аномалій програмного коду, що буде адекватний вихідним специфікаціям, може бути вирішена використанням відомої ідеології структурного програмування [2,3]. Разом з відомими перевагами (ієрархічність, наглядність, тощо), які надає застосування структурного програмування для скорочення термінів проектування, існує можливість введення контролю на рівні керуючих структур. Такі самоконтрольовані структури є базою всеосяжного ієрархічного програмного контролю. Дотримання принципу незалежності, коли структури нижнього рівня не впливають на верхні рівні, дозволяє не тільки пошарово проектувати та модифікувати СПЗ, але і побудувати наступну ієрархію локалізації помилок: процес – задача – ядро – модуль – програма – керуючі структури.

Основний зміст. Предметом цієї роботи є застосування вбудованого контролю для виявлення та діагностування помилки, пов'язаної із порушенням правильності послідовного виконання елементів програмного забезпечення.

Перевірка нелегальних виходів на неіснуючу гілку (помилкова передача управління при збої) виконується вставленням паролю (П:=1) при входженні в структурний елемент *S* і перевіркою при виході з нього з наступним обнуліннням (рис. 1).

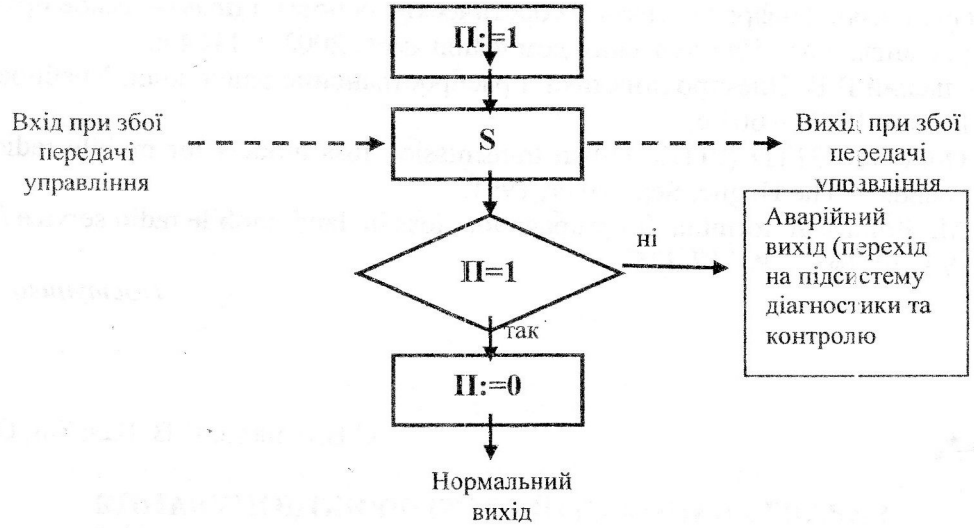

Рис.1. Використаня паролів для діагностики збоїв при передачі управління

Відсутність збігу значень паролю на виході із структури свідчить про нелегальність входження в неї (передачу управління повз вхідну точку) і призводить до ініціації діагностичної задачі, яка перевіряє паролі всіх структур. Оснащення таким захистом всіх шарів програмного забезпечення, починаючи з верхнього (задачі, ядра, модулі, структурні примітиви – керуючі структури) дозволяє знайти в графі паролів, який ізоморфний графу структури програмного забезпечення (рис. 2), шлях від кореневої вершини, яка помічена одиницею, до самого нижнього шару (кількість шарів залежить від потрібного ступеня деталізації при діагностиці та від припустимих витрат на надмірність), виявляючи елемент, в якому стався збій (чий пароль, як наслідок, не є обнуленим).

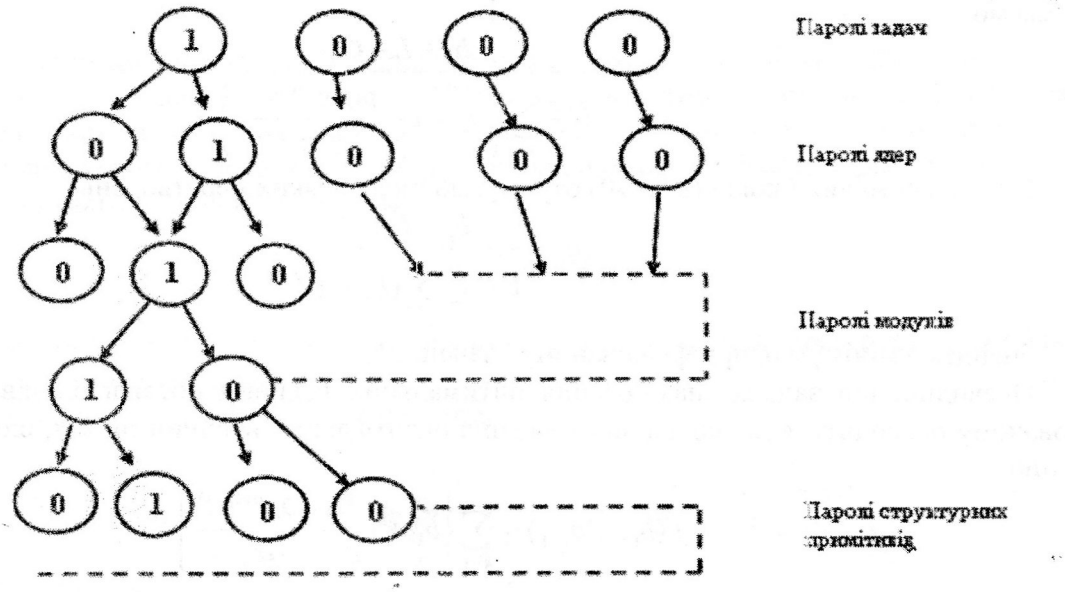

Рис.2 Граф полів

Формулу для вибору раціонального розміру захищених блоків можна отримати на підставі таких міркувань.

Введемо позначення:

b_i – кількість машинних команд в блоці M_i, який захищений паролем $П_i$;

α – ймовірність збою при виконанні команди (з урахуванням циклів);

l – кількість машинних команд, що необхідна для реалізації одного паролю;

L – додаткова пам'ять, яка потрібна для реалізації метода паролів;

$$L \geq nl,$$

n – кількість паролів;

B – пам'ять, що захищена паролями;

$$B = \sum_{i=1}^{n} b_i ,$$

q_i – умовна ймовірність не визначення збою при передаванні управління системою $П_1$, ..., $П_n$ при умові, що збій мав місце в блоці M_i;

q – безумовна ймовірність не визначення програмного збою системою паролів $П_1$, ..., $П_n$ (безвідносно до того або іншого блоку);

C – обсяг пам'яті, не захищений системою паролів;

V – загальний обсяг пам'яті, $V = B + C + L$.

Зрозуміло, що

$$q_i = \frac{b_i + L + C}{B + C + L} + p_i \frac{b_i + L + C}{B + C + L} + \ldots + p_i^n \frac{b_i + L + C}{B + L + C} = \frac{b_i + L + C}{V(1 - p_i)}$$

Тут p_i – спільна ймовірність того, що при випадковому збої в блоці M_i управління передається іншому блоку, але збій не буде викритий паролем, який відповідає черговому (після збою) блоку (до якого потрапило управління) через виникнення чергового збою у зазначеному блоці.

$$p_i = \sum_{k \neq i} \frac{b_k}{V} \left(\frac{1}{b_k} \sum_{r=o}^{b_k} [1 - (1 - \alpha)^r] \right) = \frac{1}{V} \sum_{k \neq i} \left[(b_k + 1) - \frac{1 - (1 - \alpha)^{b_k + 1}}{\alpha} \right].$$

Формули можна спростити при припущеннях, що не мають протиріч із практикою. При $\alpha \to 0$ маємо

$$q_i = \frac{b_i + L + C}{V - \sum_{k \neq i} \left(b_k + 1 - \frac{1 - \lambda^{-\alpha(b_k+1)}}{\alpha} \right)}.$$

У випадку малих блоків ($\alpha b_k \to 0$) отримуємо після деяких перетворень

$$q_i = \frac{b_i + L + C}{V - \frac{\alpha}{2} \sum_{k \neq i} (b_k + 1)^2}.$$

Знайдемо мінімум q_i при фіксованому значенні b_i.

Очевидно, що задача знаходження оптимальних величин обсягів блоків b_k, $k \neq i$, при фіксованому b_i зводиться до задачі знаходження оптимальних величин b_k, $k \neq i$, що мінімізують функцію

$$f(b_1, \ldots, b_{k-1}) = \sum_{k=1}^{n-1} \left\{ b_k + 1 - \frac{1 - \lambda^{-\alpha(b_k+1)}}{\alpha} \right\}.$$

при обмеженнях

$$\sum_{k=1}^{n-1} b_k = B - b_i; \; b_k \geq 0.$$

Вводячи заміну $y_k = b_k + 1$ і зробивши необхідні перетворення, отримуємо систему

$$y_k = B - b_i + (n-1) - (y_1 + \ldots + y_{n-2}); \quad k = \overline{1, n-2},$$

звідки випливає

$$y_1 = y_2 = \ldots = y_{n-2}$$

і остаточно

$$b_1 = b_2 = \ldots = b_{n-2}.$$

Таким чином, ми показали, що при фіксованих n та b_i мінімум q_i досяжний у випадку рівності обсягів блоків, що підлягають охороні.

Вважаючи, що

$$b_i = B/n, \quad i = \overline{1, n}, \tag{1}$$

отримаємо при $\alpha \to 0$

$$q_i = \frac{\frac{B}{n} + L + C}{V - (n-1)\left(\frac{B}{n} + 1 - \frac{1 - \lambda^{-\alpha\left(\frac{B}{n}+1\right)}}{\alpha} \right)}, \tag{2}$$

та при $\frac{\alpha B}{n} \to 0$

$$q_i = \frac{\frac{B}{n} + L + C}{V - \frac{\alpha}{2}(n-1)\left(\frac{B}{n} + 1 \right)^2}. \tag{3}$$

Безумовна ймовірність того, що випадковий збій не буде виявлений системою паролей $\{П_i\}$, дорівнює

$$q = \frac{b_i}{B}\sum_{i=1}^{n} q_i .$$

Дійсно, оскільки відмови з ймовірністю α являють собою рідкі події (α→0), можна стверджувати (із посиланням на теорему Пуассона і властивості експоненційного закону розподілу), що моменти виникнення збоїв розподілені рівномірно, тобто ймовірність надходження випадкового збою в модулі M_i (при умові, що збій відбувся) дорівнює b_i/B.

Беручи до уваги вираз (1), отримаємо

$$q = \frac{1}{n}\sum_{i=1}^{n} q_i = q_i .$$

Знайдемо оптимальну кількість захищених блоків, при якій досягається найбільший ефект від захисту, тобто $q_i = q_{i\min}$.

Підставляючи $L = nl$ у вираз (3), отримаємо

$$q_i = \frac{\frac{B}{n} + nl + C}{B + nl + C - \frac{\alpha}{2}(n-1)\left(\frac{B}{n}+1\right)^2} = \frac{an^3 + bn^2 + cn}{dn^3 + en^2 + fn + g},$$

де $a = 2l$, $b = 2C$, $c = 2B$, $d = 2l - \alpha$, $e = 2B + 2C + 2\alpha B + \alpha$, $f = 2\alpha B - 2\alpha B^2$, $g = 2\alpha B^2$.

Звідси оптимальне n вираховується з рівняння

$$a_4 n^4 + a_3 n^3 + a_2 n^2 + a_1 n + a_0 = 0.$$

де $a_4 = 2l[2B + 4l + \alpha(2B+1)] - 2\alpha C$,

$a_3 = 4B\{\alpha[l(2 - B) + 1] - 2l\}$,

$a_2 = 2B\{\alpha[B(3l - C - 2) + 2C] - 2(B + C) - \alpha\}$,

$a_1 = 2\alpha B^2(2C - B - 2)$,

$a_0 = 2\alpha B^2$.

Більш зручну формулу можна отримати, використовуючи вираз (2).

При α→0 маємо $q_i = \dfrac{\frac{B}{n} + nl + C}{B + C + nl - (n-1)\left(\frac{B}{n} + 1 - \frac{1 - \lambda^{-\alpha(\frac{B}{n}+1)}}{\alpha}\right)}$.

Після деяких перетворень отримуємо остаточно

$$n^* = 1 + \sqrt{1 + \frac{B + C}{l}}. \qquad (4)$$

З метою перевірки отриманої формули був проведений такий експеримент.

Для лінійної програми обсягом B, записаної з абсолютної адреси AA, проводилися такі дії.

Крок 1. В програмі встановлюється n паролів. Обсяг пам'яті, що захищається паролями, дорівнює $B + 10n$. Обсяг захищеного блоку дорівнює B/n. На першому кроці $n = 2$.

Крок 2. Генерується випадкове число, розподілене за псевдорівномірним законом в інтервалі $AA \div B+10n$. Позначимо його через S.

Крок 3. За допомогою генератора отримуємо число, розподілене за псевдо рівномірним законом в інтервалі $AA \div B + 10n$. Нехай це буде число g.

Крок 4. В програмі встановлюється n паролів, що захищають блоки розміру B/n.

Крок 5. В програму вноситься збурення: в чарунку пам'яті з адресою S вноситься команда JMP g.

Крок 6. Здійснюється прогін програми і за допомогою пакета „PAROL" провадиться намагання виявити помилку.

Кроки 2 ÷6 реалізуються 100 разів.

Крок 7. Встановлюється нове значення $n_{i+1} = 2n_i$.

Реалізується описана процедура.

Результати експерименту для програм обсягом ≈10К і 4К подані у таблицях 1 та 2, відповідно. Розрахунок за формулою (4) для вихідних даних B = 10К, l = 10 дає n^* = 32, для даних B = 4К, l = 10 дає n^* = 21.

Таблиця 1

Кількість паролів	Кількість виявлених помилок
2	47
4	70
8	88
16	92
32	95
64	93
128	86
256	73
B = 10К, l = 10, n^* = 32	

Таблиця 2

Кількість паролів	Кількість виявлених помилок
2	52
4	77
8	85
16	90
32	88
64	83
B = 4К, l = 10, n^* = 21	

Як видно з таблиць, результати експерименту співпадають із розрахунковими даними з достатньою для практичного застосування точністю.

Список літератури

1. *Сбитнев А.И.* Структурные методы проектирования математического обеспечения АСУ ТП// Модели и алгоритмы автоматизированных систем в промышленности. – К.: ИК АН УССР, 1982. – С. 3-9.
2. *Лєнков С.В., Вишнівський В.В., Перегудов Д.О., Толюпа С.В.* Методика розрахунку часу затримки інформації управління в мережах при випадковому потоці повідомлень // Вісник державного університету інформаційно-комунікаційних технологій. – К., 2007.- №5(4). – С. 10 – 18.
3. *Грищак О.М.* Пропозиції до перспективної структури підрозділу, що розробляє спеціальне програмне забезпечення военного призначення // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К., 2007. – № 8. – С.61 -66.

Надійшла 26.03.2008р.

УДК 004.056.5: 518

А.А.Кобозева, В.А Хорошко

ВЕКТОРНАЯ SIGN-ЧУВСТВИТЕЛЬНОСТЬ КАК ОСНОВА ГЕОМЕТРИЧЕСКОЙ МОДЕЛИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

1. Введение

Процесс внедрения новых информационных технологий во все сферы жизни общества немыслим без решения вопросов информационной безопасности. Современное общество вступает в постиндустриальный период своего развития, который по всеобщему мнению можно назвать информационным [1].

Создание интенсивной системы комплексного обеспечения безопасности информационных технологий невозможно без обобщения накопленного опыта теоретических исследований и практического решения задач защиты информации, т.е. без развитого научного базиса [2,3], создание которого немыслимо без разработки адекватной математической модели системы защиты информации (СЗИ). В современных публикациях данному вопросу уделено много внимания [2,4-6], однако предложенные формализации не удовлетворяют всем выдвигаемым к математической модели СЗИ требованиям, являются, как правило, достаточно сложными в вычислительном смысле [5,6], что безусловно связано с тем, что теоретические основы построения СЗИ исключительно сложны и, несмотря на интенсивность исследований в этой предметной области, еще далеки от совершенства [2].

В [7] предложена модель СЗИ, основывающаяся на принципах функционирования нервной системы человека. Математическими инструментами для ее создания явились теория графов, матричный анализ и теория возмущений. Применение теории возмущений позволило производить априорную оценку адекватности моделируемой СЗИ предполагаемому противнику [8], дало возможность для определения чувствительности совокупной системы к возмущающим воздействиям (атакам). Настоящая работа является дальнейшим развитием предложенного в [7] подхода, использующего чувствительность информационного объекта для определения его свойств.

Любая атака, действующая на информационно-технологическую систему (ИТС), на каждом из имеющихся в распоряжении СЗИ средств защиты отразится по-разному: некоторые из средств могут быть разрушены полностью, некоторые выведены из строя частично, а для каких-то средств атака окажется безопасной.

Целью настоящей работы является создание основ модели СЗИ, дающей возможность простого в вычислительном смысле учета различий в результатах воздействия атаки для разных средств защиты, следствием чего в перспективе должно стать значительное упрощение решения задачи по установлению адекватности СЗИ предполагаемому противнику по