УДК 004.492.3

С.М. ЛИСЕНКО, А.П. ГОНТАР, А.С. ШЕВЦОВ
Хмельницький національний університет

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ РЕАЛІЗАЦІЇ ІНТЕЛЕКТУАЛЬНОГО МЕТОДУ ПОШУКУ ТРОЯНСЬКИХ ПРОГРАМ В ПЕРСОНАЛЬНИХ КОМП'ЮТЕРАХ

В роботі розроблено програмне забезпечення виявлення невідомих троянських програм в персональних комп'ютерах, що ґрунтується на інтелектуальному методі їх пошуку шляхом використання нечіткої логіки та алгоритмів штучних імунних систем. Досліджено результати роботи розробленого програмного забезпечення.

Exposure of the unknown trojan programs software is in-process developed in the personal computers, that is based on the intellectual method of their search by the use of fuzzy logic and algorithms of the artificial immune systems. Investigational job of the developed software performances.

Ключові слова:

Вступ

Дослідження методів та програмного забезпечення (ПЗ) пошуку троянських програм (ТП) показало низьку достовірність антивірусного діагностування (АД) [1]. Сучасне антивірусне програмне забезпечення в своїй основі ґрунтується на використанні антивірусних баз, які поповнюються вже після виявлення шкідливого ПЗ і не здатні виявляти нові невідомі троянські програми. Антивірусне програмне забезпечення (АПЗ), яке використовує евристичні методи пошуку поки демонструють недостатню достовірність АД. В роботах [2-6] представлені новий інтелектуальний метод пошуку ТП в ПК, яки ґрунтуються на використанні інтелектуальних компонент, а саме нечіткої логіки та алгоритмів штучних імунних систем (ШІС).

Постановка задачі

Постає науково-практична задача дослідження можливості практичної програмної реалізації інтелектуального методу. Також необхідним є дослідження результатів роботи розробленого ПЗ щодо спроможності підвищення достовірності антивірусного діагностування із застосуванням даного методу.

Програмне забезпечення пошуку ТП в ПК

Для ефективної організації процесу пошуку троянських програм в персональних комп'ютерах було розроблено програмне середовище, яке забезпечує мінімум трудозатрат користувача при його експлуатації ПК. При розробці антивірусного програмного забезпечення використовувались принципи структурного програмування згідно яких проектування та від лагодження програмних одиниць виконується за правилами програмування «зверху вниз», де процес написання ПЗ починається з визначення ієрархії в структурі ПЗ та поступової деталізації програми у вигляді сукупності підпорядкованих програмних модулів. Даний спосіб забезпечує можливість модифікаціїї програмного коду, оскільки зміни в одному із модулів, не вимагає перекопіляції усіх інших модулів розроблюваного програмного забезпечення.

Розроблені програмні засоби реалізації інтелектуального методу пошуку ТП в ПК дають змогу здійснити основні операції антивірусного діагностування ПК та налагоджуватися згідно вимог користувача.

Програмне забезпечення надає користувачу наступні можливості:

- виконати запуск антивірусного монітора, який відслідковуватиме системні події та має змогу виявляти підозрлі програмні обєкти в середовищі операційної системи;
- виконати антивірусне сканування персонального комп'ютера на предмет підміни системних файлів троянськими версіями.

При розробці програмного забезпечення використовувалась мови програмування С, С++ із застосування середовища розробок програмних продуктів C++Builder 7.0 [7]. Також в програмній реалізації було використано модуль з пакету fuzzy logic toolbox, що входить до складу прикладного програмного забезпечення для вирішення технічних Matlab 7.0 [8].

ПЗ системи пошуку ТП в ПК (СПТП) включає дві частини ПЗ: користувацьку і адміністраторську.

Користувацька частина передбачає можливість проведення антивірусного моніторингу системи, що діагностується. Користувач має змогу запустити антивірусний монітор чи відключити його.

Також користувацька частина програмного забезпечення передбачає можливість проведення антивірусного сканування ПК за вимогою користувача для виявлення системних файлів, що можуть бути троянськими модифікаціями та виконувати деструктивні дії в операційній системі.

Розроблена СПТП дає змогу користувачу здійснити оновлення антивірусних баз для забезпечення підвищення достовірності антивірусного діагностування ПК.

Адміністраторська частина передбачає можливість спеціалісту (чи спеціалістам) виконати формування (редагування) антивірусних баз, що використовуються в моніторі та сканері. Формування баз для монітора полягає в занесенні поведінкових моделей троянських програм на різних етапах їх життєвого циклу (ЖЦ).

Антивірусні бази для сканера створюються шляхом вибірки файлів для сканування, генерації захищених двійкових послідовностей та детекторів.

Структурні схеми ПЗ СПТП користувацької та адміністраторської частин подано на рис. 1.

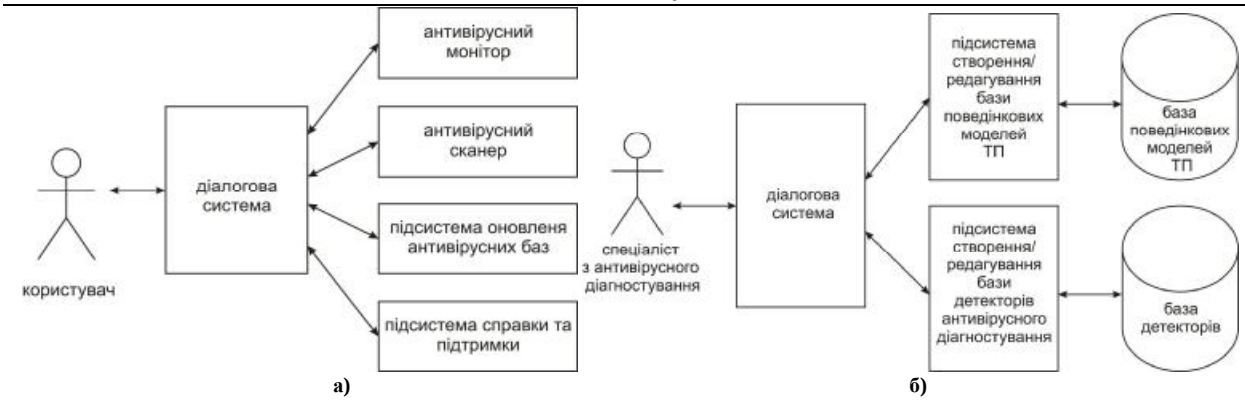


Рис. 1. Структурні схеми ПЗ СПТП: а) користувацька частина, б) адміністраторська частини

За допомогою діалогової підсистеми користувач системи пошуку троянських програм має змогу виконати запуск антивірусного монітора, який буде виконувати постійне відслідковування системних подій програмних об'єктів в ПК на предмет їх схожості на ТП. Таких пошук система АД веде в базі поведінок ТП.

База поведінок включає три складові бази: базу поведінок ТП на етапі потрапляння, базу поведінок ТП на етапі активізації та базу поведінок ТП на етапі виконання закладених функцій. Пошук здійснюється по хешу та знаходженні максимально відповідної поведінки троянській програмі.

У випадку виявлення схожого програмного об'єкту на ТП, зібрана інформація передається на систему нечіткого логічного висновку, яка присутня в складі СПТП і призначена для виконання результуючого рішення щодо можливості присутності ТП в ПК. Таким результатом є число від 0 до 1, яке свідчить про ступінь підозрілості досліджуваного програмного об'єкту. Згідно з вибраною політикою безпеки, а саме вибору порогу активізації підсистеми блокування дій підозрілого ПЗ, користувач буде сповіщений про підозріле ПЗ та запропоновано підтвердити продовження роботи даного ПЗ чи заблокувати його роботу.

Додатково за допомогою діалогової підсистеми користувач системи пошуку троянських програм має змогу виконати запуск антивірусного сканера, який може здійснити виявлення факту підміни системних файлів троянськими версіями. Для цього користувач може виконати вибір файлів для антивірусного сканування за його типом чи просто вибравши необхідна каталоги файлів.

СПТР в своєму складі має підсистему поновлення баз поведінок троянських програм. Для цього користувач вибирає необхідну вкладку в АПЗ і натискає кнопку «завантажити антивірусні оновлення». В склад СПТП також входить підсистеми довідки для пояснення користувачу як користуватися розробленою системою антивірусного діагностування персонального комп'ютера.

Адміністраторська частина розробленого програмного забезпечення пошуку ТП в ПК призначена для спеціалістів в області антивірусного діагностування, які мають великий досвід у дослідженнях поведінки шкідливого програмного забезпечення. Розроблене ПЗ дає можливість створення поведінкових моделей та занесення їх до спеціальної антивірусної бази, яка потім використовуватиметься користувачами для антивірусного діагностування ПК.

Загалом є дві окремі антивірусні бази: для моніторингу та сканування. База, що використовується для моніторингу представляє собою три БД, для кожного з етапів життєвого циклу ТП в ПК. Кожна поведінка, яка заноситься спеціалістом є матрицями відповідності між діями програмного об'єкту і системними портами, та матрицями відповідності між діями ТП і структурними одиницями ОС ПК. З кожної поведінки формується хеш, за яким в подальшому виконується пошук ТП.

База, що застосовується для сканування ПК використовує розроблені підсистеми, які спочатку виконують формування набору файлів для сканування, а потім виконують генерацію антивірусних детекторів. БД антивірусного сканера представляє собою сховище двійкових послідовностей для кожного відібраного файлу та сформованих детекторів.

Адміністратор СПТП має додатково змогу здійснювати налаштування в формуванні детекторів шляхом підбору параметрів генерації детекторів, а саме: у виборі кількості необхідних детекторів, розрядності детекторів та ключа пошуку. Перераховані параметри впливають на швидкість сканування та ймовірність виявлення факту підміни системних файлів троянськими версіями. Функційні схеми користувацької та адміністраторської частин програмного забезпечення СПТП в ПК показані на рис. 2.

Весь програмний комплекс СПТП складається з п'яти частин:

- системи запуску антивірусного діагностування trojan_finder,
- антивірусного монітора (АМ) – monitor (користувацька частина);
- антивірусного сканера (АС) – scaner (користувацька частина);
- підсистеми створення та редагування баз поведінок ТП – editor (адміністраторська частина);
- генератора антивірусних детекторів – detector (адміністраторська частина).

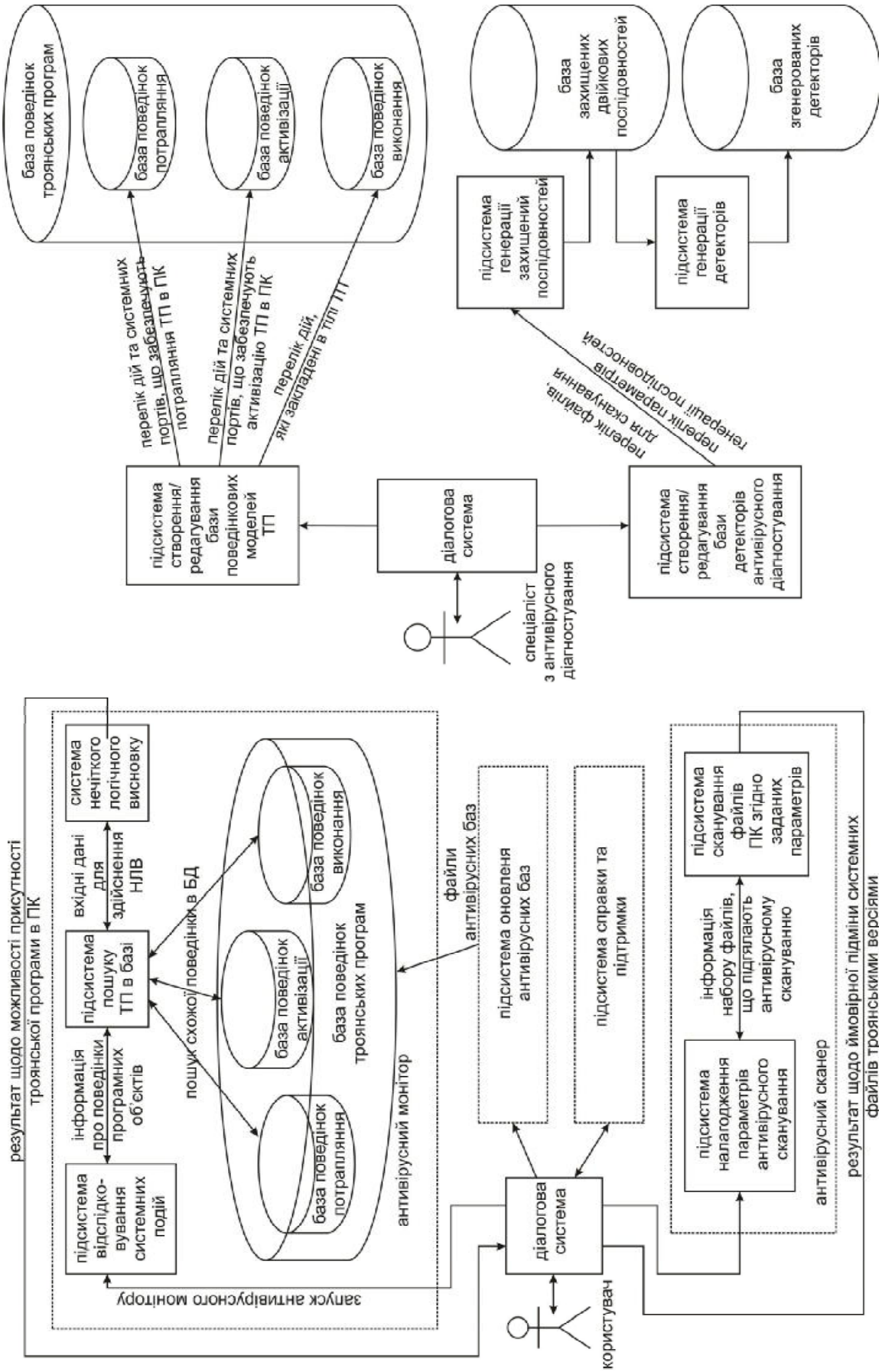


Рис. 2. Функційні схеми ПЗ СПТП: а) користувацька частина, б) адміністраторська частини

Система запуску антивірусного діагностування trojan_finder є основною в складі СПТП, оскільки призначена для запуску, зупинки та налаштування параметрів АД. Дана система викликає модулі антивірусного монітора та сканера та керує їх роботою. Опис модулів, які входять до складу системи trojan_finder подано в таблиці 1. До складу антивірусного монітора входять модулі, перелік яких подано в таблиці 2.

Таблиця 1

Опис модулів системи trojan_finder

Назва модуля	Призначення
trojan_finder.cpp	модуль керування системою діалогу з користувачем
Unit1.cpp	модуль запуску, зупинки та комплексу АД; виклик монітора та сканера; виконання оновлення баз; запуск довідки роботи комплексу

Таблиця 2

Модулі програмного забезпечення антивірусного монітора

Назва модуля	Призначення
monitor.cpp	основна програма функціюванням монітора, яка ініціалізує діалогову систему монітора та викликає інші модулі
unit_monitor.h	модуль, який виконує моніторинг за системними подіями, здійснює пошук схожих поведінок у БД за їх хешем
cmp.h	порівняння згенерованої поведінки з поведінками з наявної антивірусної бази
hash.h	створення хешу та виконання пошуку за заданими ключами
memory.h	виділення пам’яті для створення хешу
table.h	перебір поведінкових моделей
types.h	робота з антивірусними базами
fis.h	модуль обробки параметрів fis-файлів, що завантажуються в середовище АМ
fuzzy.h	модуль здійснення НЛВ щодо можливості присутності ТП в ПК
backdoor.h	модуль бази поведінкових моделей ТП типу backdoor
trojan-PSW.h	модуль бази поведінкових моделей ТП типу trojan-PSW
trojan-Clicker.h	модуль бази поведінкових моделей ТП типу trojan-Clicker
trojanDownloader.h	модуль бази поведінкових моделей ТП типу trojan-Downloader
trojanDropper.h	модуль бази поведінкових моделей ТП типу trojan-Dropper
trojanProxy.h	модуль бази поведінкових моделей ТП типу trojan-Proxy
trojanSpy.h	модуль бази поведінкових моделей ТП типу trojanSpy
trojanNotifier.h	модуль бази поведінкових моделей ТП типу backdoor

Опис роботи модулів, які входять до складу антивірусного сканера представлено в таблиці 3. Опис модулів, які входять до складу системи формування баз поведінок троянських програм подано в таблиці 4. Опис модулів, які входять до складу системи генерації детекторів подано в таблиці 5.

Таблиця 3

Модулі, які входять до складу антивірусного сканера

Назва модуля	Призначення
scanner.cpp	модуль діалогової системи антивірусного сканера з користувачем
Unit1.cpp	модуль виконання сканування шляхом перебору збігу захищених двійкових послідовностей зі згенерованими детекторами
Data.h	модуль генерації детекторів
Db.h	модуль читання з баз даних детекторів
String.h	модуль обробки двійкових послідовностей
Table.h	модуль читання таблиць
Type.h	модуль передачі параметрів сканування

Таблиця 4

Модулі системи побудови БД поведінок ТП

Назва модуля	Призначення
editor.cpp	модуль керування системою діалогу з адміністратором СПТП
Unit1.cpp	Заповнення та формування таблиць
Unit2.cpp	Виконання доступу та пошук по таблицях
hash.h	створенная хешу та виконання пошуку за заданими ключами
memory.h	виділення пам’яті для створення хешу
table.h	перебір поведінкових моделей
types.h	робота з антивірусними базами

Таблиця 5

Модулі, які входять до складу системи генерації детекторів

Назва модуля	Призначення
detector.cpp	модуль керування системою діалогу з з адміністратором СПТП
Unit1.cpp	модуль створення відбитків файлів
Unit2.cpp	Модуль створення детекторів

Для забезпечення функціюванням в програмному середовищі операційних систем Windows XP, Windows Vista і Windows 7 для кожного з п'яти основних модулів розробленого програмного забезпечення було використано динамічні бібліотеки: Rtl60.bpl, Vcl60.bpl, Vcl.bpl, Borlandmm.dll, Cc3260mt.dll, dbeditorpp.dll.

Програмні засоби розроблення системи нечіткого логічного висновку

Складовою антивірусного монітору, який реагує на підозрілі програмні об'єкти є підсистема аналізу та висновку. В основі даної підсистеми лежить використання розробленої системи нечіткого логічного висновку (СНЛВ). Для ророоблення такої СНЛВ було використано програмний засіб Fuzzy Logic Toolbox з пакету Matlab 7, який є набором інструментів для побудови та аналізу нечітких множин [8].

Система нечіткого логічного висновку, яка входить до складу антивірусного монітора, в розробленому програмному забезпеченні реалізована у вигляді програмних модулів fis.h та fuzzy.h, які зчитують та опрацьовують спеціальну структуру даних, що представляється в робочій області пакету MatLab у вигляді fis-файлів – текстових файлів спеціального формату.

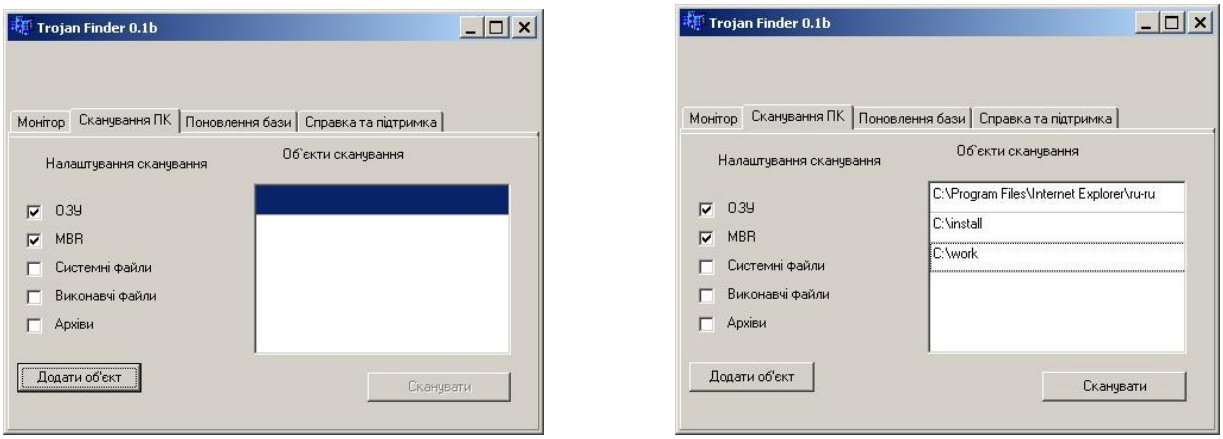
Для визначення ступеня підозрілості програмного об'єкту в адміністративній частині програмного забезпечення пошуку ТП в ПК існує можливість завантаження попередньо налаштованого спеціалістами антивірусного діагностування ПК fis-файлу.

Інтерфейс програмного забезпечення

Результатом компіляції описаного вище проекту є прикладне програмне забезпечення з інтерфейсом, представленим на рисунках 3-10.

а) **б)**

Рис. 3. Антивірусний монітор: а) зупинений монітор, б) запущений монітор



а) **б)**

Рис. 4. Антивірусний сканер: а) параметри сканування, б) файли для сканування

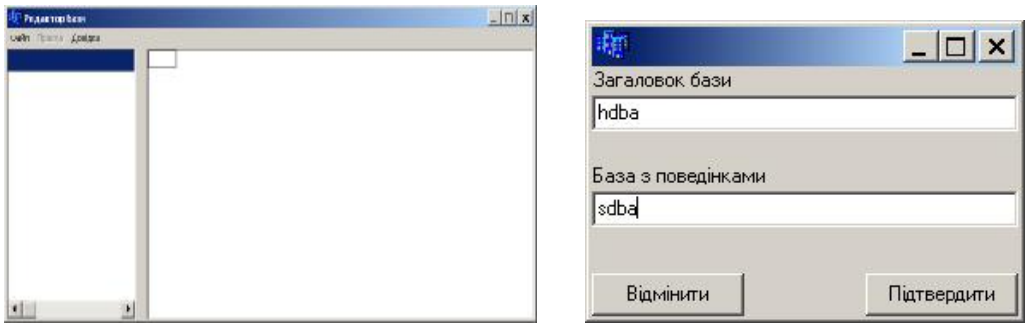
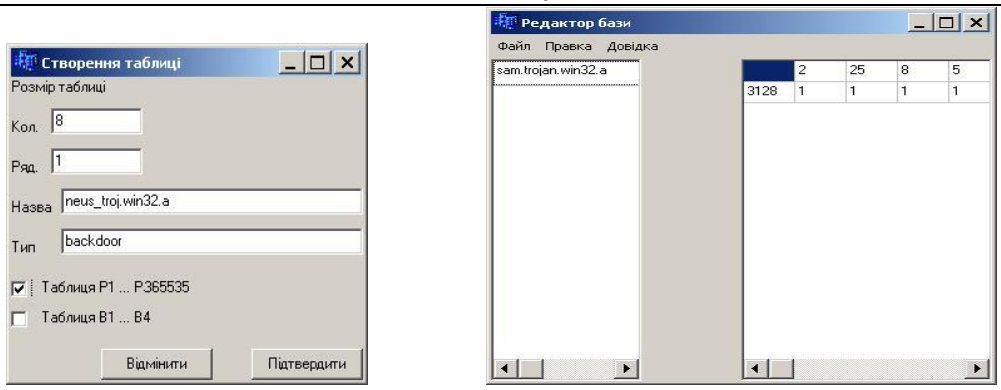
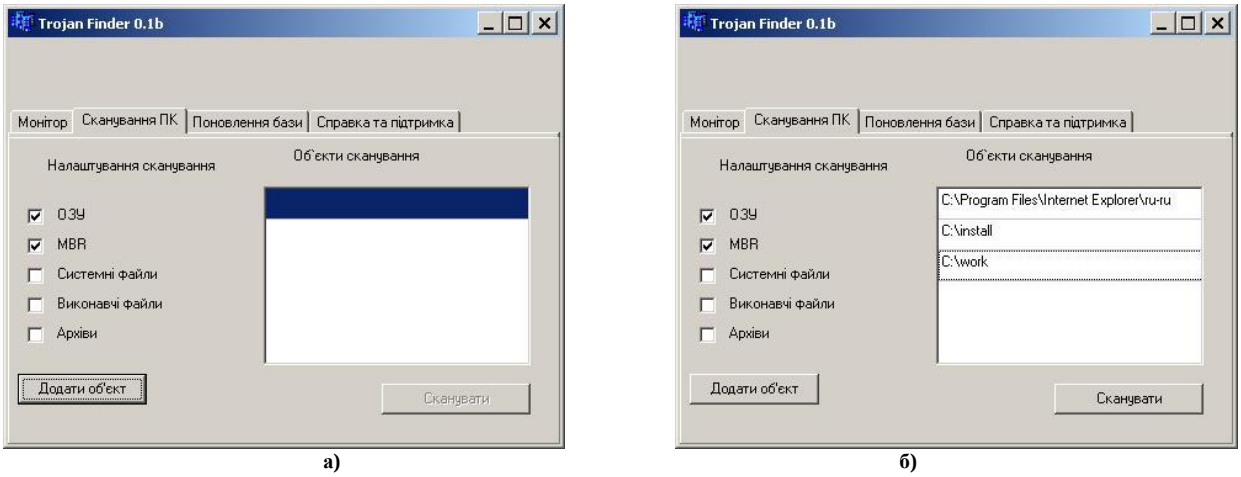


Рис. 5. Редактор баз поведінок троянських програм



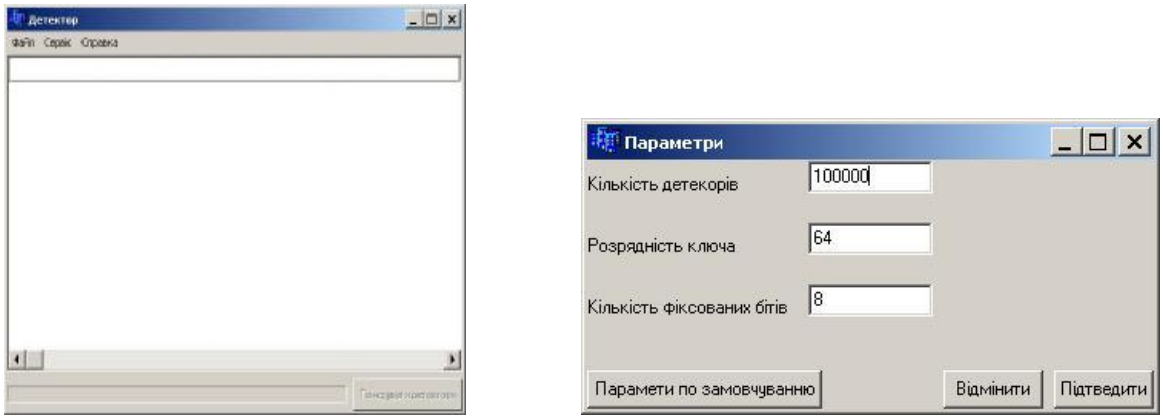
а) **б)**

Рис. 6. Редактор баз поведінок троянських програм: а) створення таблиць, б) відображення поведінки троянської програми



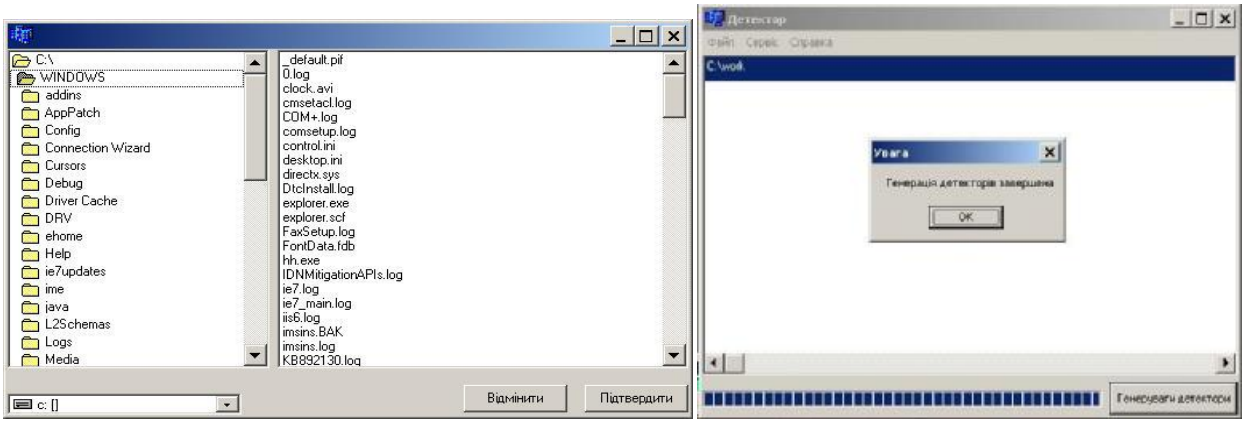
а) **б)**

Рис. 7. Антивірусний сканер: а) параметри сканування, б) вибір файлів для сканування



а) **б)**

Рис. 8. Редактор детекторів антивірусного сканування: а) загальне вікно, б) параметри створення детекторів



а) б)

Рис. 9. Генератор детекторів: а) вибір файли для створення захищених послідовностей, б) генерація детекторів

Результати антивірусного діагностування програмного забезпечення

Для демонстрації роботи програмного забезпечення було програмно згенеравано 324 програмних об'єкти з функційним навантаженням троянських програм. Дані програми потенційно невідомі для антивірусних баз фірм-розробників антивірусного ПЗ.

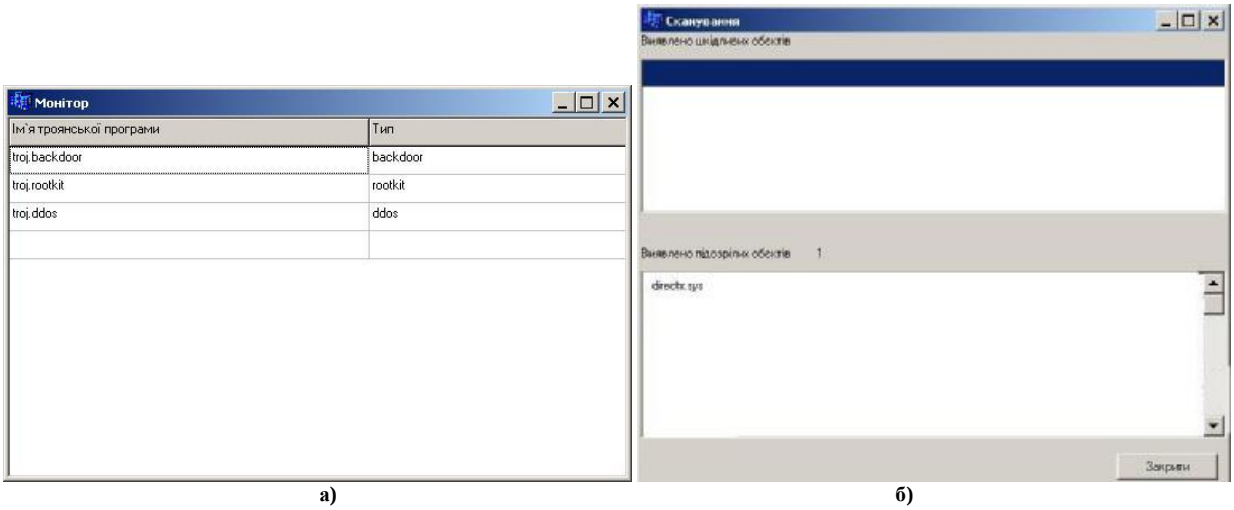
В своїй основі набір згенерованого ПЗ має такі властивості:

- 18 програм використовують rootkit-технологію
- 81 програм мають функційне навантаження ТП типу BackDoor
- 32 програм мають функційне навантаження ТП типу Trojan-PSW
- 21 програм мають функційне навантаження ТП типу Trojan-Clicker
- 85 програм мають функційне навантаження ТП типу Trojan Downloader
- 23 програм мають функційне навантаження ТП типу Trojan-Dropper
- 15 програм мають функційне навантаження ТП типу Trojan-Proxy
- 33 програм мають функційне навантаження ТП типу Trojan-Spy
- 16 програм мають функційне навантаження ТП типу Trojan-Notifier

Чисельне співвідношення згенерованих програм відповідає процентному співвідношенню типів троянських програм, які найчастіше інфікують персональні комп'ютери.

З вказаного набору 8 програмних об'єктів виконували підміну системних файлів, але не виконували деструктивних дій на ПК.

Результати антивірусного діагностування із залученням розробленого ПЗ подано в таблиці 4.7 та на рис. 10.



а) **б)**

Рис. 10. Результати антивірусного діагностування ПК: а) антивірусного монітора, б) антивірусного сканера

Результати роботи програмної реалізації системи пошуку троянських програм демонструють спроможність виявлення троянських програм із застосуванням компонентів штучного інтелекту. Так із згенерованого набору програмних об'єктів видно виявлення антивірусним монітором поведінки, що занесені до бази і найбільше «схожі» до троянських програм типів backdoor, rootkit та ddos. Антивірусне сканування ПК виявило модифікацію системного файлу directx.sys.

Таблиця 6

Результати антивірусного діагностування із залученням розробленого ПЗ

Програми з властивостями троянських програм типу		Кількість програм, ідентифікованих як підозрілі	Відсоток виявлення, %
Rootkit	18	10	55,55
BackDoor	81	75	92,59
Trojan-PSW	32	25	78,12
Trojan-Clicker	21	8	38,09
Trojan Downloader	85	67	78,82
Trojan-Dropper	23	13	56,52
Trojan-Proxy	15	10	66,67
Trojan-Spy	33	23	69,69
Trojan-Notifier	16	9	56,25
Всього	**324**	**240**	**74,07**

Дослідження розробленого програмного забезпечення показали приріст параметра достовірності антивірусного діагностування ПК в 5-15 % у порівнянні з існуючими засобами АПЗ.

Висновки

В результаті проведеного дослідження було розроблено програмне забезпечення, яке реалізує

інтелектуальний метод пошуку троянських програм в ПК. Розроблене програмне забезпечення реалізує процес виявлення троянських програм в персональних комп'ютерах, який ґрунтується на використанні нечіткої логіки для здійснення антивірусного моніторингу та застосуванні алгоритмів штучних імунних систем для реалізації антивірусного сканування персональних комп'ютерів.

Дослідження результатів програмної реалізації інтелектуального методу пошуку ТП в ПК показало можливість здійснення антивірусного діагностування ПК з ймовірністю 75 %, що є високим результатом для виявлення нових невідомих троянських програм.

Розроблене програмне забезпечення дозволяє здійснювати виявлення відомих та невідомих троянських програм в персональних комп'ютерах без побудови баз сигнатур вірусних програм.

Література

1. Савенко О.С., Лисенко С.М. Дослідження методів антивірусного діагностування комп'ютерних мереж // Вісник Хмельницького національного університету. – 2007. – № 2, Т.2. – С.120-126.

2. Савенко О. Розробка процесу виявлення троянських програм на основі використання штучних імунних систем / Олег Савенко, Сергій Лисенко // Вісник Хмельницького національного університету. – 2008. – № 5, – С.183-188.

3. Савенко О.С. Использование нечеткой логики для поиска троянских программных продуктов в вычислительных системах/ Савенко О.С., Графов Р.П., Лисенко С.М // Вісник Чернівецького національного університету. – 2009. – № 6, – С.25-31.

4. Савенко О. Лисенко С. М. Інтелектуальний метод та алгоритми пошуку троянських програм в персональних комп'ютерах / Олег Савенко, Сергій Лисенко // Вісник Вінницького політехнічного інституту. – 2008. – № 6, – С.129-137.

5. Савенко О. Алгоритми пошуку троянських програм в персональних комп'ютерах / Олег Савенко, Сергій Лисенко // Радіоелектронні і комп'ютерні системи. – 2009. – № 6. – С.98-103.

6. Borland C++ Builder 6. Руководство разработчика / Джаррод Холингворт, Боб Сворт, Марк Кэшмэн, Поль Густавсон. – М.: Вильямс, 2004. – 976 с.

7. Штовба С.Д. Проектирование нечетких систем средствами MATLAB. – М.: Горячая Линия – Телеком, 2007. – 288 с.

Надійшла 5.12.2009 р.

УДК 681.3+519.6

О.А. ПАСТУХ
Європейський університет

ЧИСЕЛЬНЕ МОДЕЛЮВАННЯ ПРЕДСТАВЛЕННЯ ГРАФІВ З НЕЧІТКИМИ МІТКАМИ В КВАНТОВИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Вперше здійснено чисельне моделювання представлення графів з нечіткими мітками у квантових нечітких інформаційних системах другого роду за допомогою квантових нечітких відношень другого роду. Основу моделювання складає мікропрограма в унітарно-операторній формі, що діє на сімейство квантових процесорів квантової нечіткої інформаційної системи другого роду. Правильність результатів моделювання встановлена шляхом проведення перевірки, яка полягає в порівнянні результатів чисельного моделювання на основі нечітких відношень та на основі квантових нечітких відношень другого роду в квантових нечітких інформаційних системах другого роду.

Numerical simulation of graph with fuzzy marks in the quantum fuzzy information systems of second level had been realized. Quantum fuzzy relations of second level are basic of numerical simulation. Micro program at unitary-operator form is for sets of quantum processors of quantum fuzzy information systems of second level. Results of numerical simulation fuzzy relations and results of numerical simulation quantum fuzzy relations of second level in the quantum fuzzy information systems of second level had been compared.

Ключові слова: графи, нечітка мітка, інформаційна система.

Вступ. Як відомо [1, 2], графи широко використовуються при розв'язуванні найрізноманітніших задач у сфері інформаційних технологій. Серед великої сукупності різного типу графів чинне місце займають графи з нечіткими мітками.

Одним з актуальних питань, яке пов'язане з графами із нечіткими мітками є питання їх представлення в квантових інформаційних системах, зокрема, в квантових нечітких інформаційних системах другого роду ($q_{II} f$ -системах).

Огляд існуючих відомостей. В основі представлення графів з нечіткими мітками у $q_{II} f$ -системах лежать квантові нечіткі множини, які вперше введені автором у його роботах [3-6].

Мета. Здійснити чисельне моделювання представлення графів з нечіткими мітками у $q_{II} f$ -системах.

Постановка завдання. Чисельно змоделювати представлення графів з нечіткими мітками у $q_{II} f$ -