зрозуміло, що питання діагностування КЗ на етапі експлуатації вирішено на недостатньому рівні, ефективність рішень не задовольняє користувача КЗ. Це пов'язано з тим, що відомі експертні системи діагностування або вимагають введення тільки чіткої та точної діагностичної інформації при наповненні баз знань або лише частково допускають можливість використання нечіткої інформації, що часто не покращує, а погіршує якість рішень, що надаються у результаті. Це зумовлено недосконалістю при формалізації нечіткої діагностичної інформації у базах знань таких систем та недосконалістю алгоритмів її подальшого опрацювання. Оскільки, все ж таки, найбільш перспективним в технічній діагностиці є використання експертних систем, тому необхідно розробляти нові методи та засоби подання та опрацювання діагностичної інформації в ЕСД, що дозволить підвищити ефективність діагностування КЗ на етапі експлуатації.

Література

1. Попов Э. В. Экспертные системы 90-х гг. Классификация, состояние, проблемы, тенденции / Э. В. Попов // Новости искусственного интеллекта. – 1991. – № 2. – С. 84 – 101.

2. Скобцов Ю. А. Логическое моделирование и тестирование цифровых устройств / Ю. А. Скобцов, В. Ю. Скобцов. – Донецьк: ИПММ НАН Украины, ДонНТУ, 2005. – 436 с. – ISBN 966-02-3925-4.

3. Локазюк В. М. Інтелектуальне діагностування мікропроцесорних пристроїв та систем: [навч. посібник для вузів] / В. М. Локазюк, О. В. Поморова, А. О. Домінов. – К.: Такі справи, 2001. – 286 с.

4. Тоценко В. Г. Методы и системы поддержки принятия решений / В. Г. Тоценко // Наукова думка. – К., 2002. – 279 с.

5. Wang Z. A Combined ANN and Expert System Tool for Transformer Fault Diagnosis / Wang Z., Liu Y., Griffin P. J // IEEE Transactions on Power Delivery, Vol. 13. – No. 4. – October 1998. – P. 1224 – 1229.

6. Фрэнк Дж. Бартос. Искусственный интеллект: принятие решений в сложных системах управления / Фрэнк Дж. Бартос, CONTROL ENGINEERING.

7. Інтелектуальні інформаційні технології: ДСТУ 2481-94. – Держстандарт України. – К., 1994. – 71 с.

8. Dubois D. An introduction to possibilistic and fuzzy / Dubois D., Prade H // in N on-Standard Logics for Automated Reasoning, P. Smets et al, Eds. – New York: Academic. – 1988. – P. 287 – 326.

9. Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzyTech / А.В. Леоненков. – СПб.: БХВ – Петербург, 2003. – 736 с.: ил.

10. Герасимов Б. М. Нечеткие множества в задачах проектирования, управления и обработки информации / Б. М. Герасимов, Г. Г. Грабовський, Н. А. Рюмшин. – К.: Техніка, 2002. – 140 с.

11. Jain L. C. Hybrid Intelligent engineering systems / Jain L. C., Jain R. K. // Advances in Fuzzy Systems Applicatoins and Theory. – Vol 11. – March 1997. – 196 pp.

Надійшла 25.5.2010 р.

УДК 004.492.3

С.М. ЛИСЕНКО
Хмельницький національний університет

АДАПТИВНА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ДІАГНОСТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ НА НАЯВНІСТЬ ТРОЯНСЬКИХ ПРОГРАМ

Розроблено адаптивну інформаційну технологію діагностування комп'ютерних систем на наявність ТП, суть якої полягає у використанні розроблених поведінкових моделей класів троянських програм, відмінністю якої від відомих є те, що процес діагностування не потребує побудови баз сигнатур, дає змогу виявляти нові невідомі троянські програми та підвищує достовірність і ефективність процесу діагностування комп'ютерних систем на наявність троянських програм.

The adaptive information technology of diagnosis of the computer systems of the presence TP which uses the behavioral models of classes of TP is developed. Information technology does not need building the signature bases, can detect new TP and increases reliability and efficiency of diagnosing computer systems of the presence of TP.

Ключові слова: адаптивна інформаційна технологія, діагностування комп'ютерної системи, троянська програма, достовірність діагностування.

Вступ

Роль антивірусного програмного забезпечення в умовах тотальної інформатизації суспільства на сьогоднішній день важко переоцінити. Динамічне зростання кількості комп'ютерних систем (КС), підключення до мережі Інтернет створюють проблеми, пов'язані з їх використанням. Однією з таких проблем є розробка та поширення шкідливого вірусного програмного забезпечення, найчисленнішим класом якого сьогодні є троянські програми (ТП), діяльність яких призводить до неправильного функціонування системного програмного забезпечення та витоку конфіденційної інформації. Аналіз сучасних інформаційних технологій (ІТ) показав недостатню достовірність діагностування КС на наявність нових ТП [1], мають недоліки в швидкодії, високих вимогах до апаратного забезпечення, тому розробка інформаційної технології

діагностування КС на наявність ТП для підвищення достовірності діагностування є актуальною задачею.

Постановка задачі

Постає науково-практична задача розробки адаптивної інформаційної технології діагностування комп'ютерних систем на наявність ТП, яка б підвищила достовірність та ефективність процесу діагностування.

Актуальність задачі

Актуальність задачі діагностування КС на наявність ТП підтверджують результати дослідження співвідношення чисельності розробленого шкідливого програмного забезпечення (ШПЗ) за 2009 рік (рис. 1) та достовірності діагностування КС на наявність нових ТП КС, яка складає лише 70 % (рис. 2).

Рис. 1. Співвідношення розробленого ШПЗ за 2009 рік, класи троянських програм

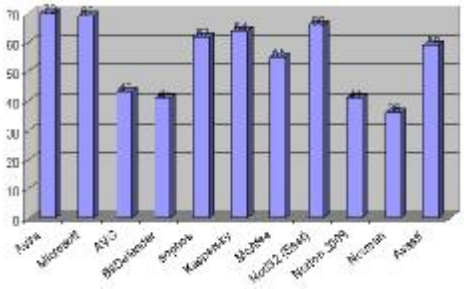


Рис. 2. Достовірність діагностування КС на наявність нових троянських програм

Поведінкова модель троянських програм

Для формалізації процесу функціонування ТП в КС було розроблено їх поведінкову модель [2]:

$$M_v = \langle \Theta, S, V, L, Aff, e \rangle,$$

де Θ – множина усіх троянських програм, S – етапи життєвого циклу (ЖЦ) троянської програми $s_i \in S$, $i = \overline{1,3}$; $V = |V_{mp}|$ – матриця відношень m дій ТП та p портів мережних протоколів; $L = |L_{ab}|$ – матриця відношень дій $a \in A$ ТП і $b \in B$ структурних одиниць ОС; e – відношення між ТП та її станами, тоді для $n \in \Theta$ та $s \in S$, відношення $n\ e\ s$ означає, що ТП ν перебуває в стані s; відношення $\nu\ \bar{\varepsilon}\ s$ означає, що ТП ν не перебуває в стані s; Aff – функція, яка визначає взаємодію між об'єктами КС і ТП n_j, тоді множина $a \in Aff(e_i, n_j)$ є набором можливих дій, які троянська програма n_j завдає об'єкту (об'єктам) e_i. Номінально, $Aff(b_i, v_j)$ є множиною впливів, які ТП e_j завдає об'єкту b_i; Z – характеристичні параметри відношень, $Z = \{z_k\}$ – вектор деструктивних дій об'єкта з нормованими пріоритетними вагами $P = \{p_k\}$, $(\sum p_k = 1)$, що враховують рівень їхньої небезпеки для КС.

На основі поведінкової моделі було побудовані поведінкові моделі ТП усіх класів. Приклад поведінкової моделі ТП класу Trojan-Backdoor подано кортежем:

$$M_{\Theta_{BD}} = \langle \Theta_{BD}, A_{BD}, B_{BD}, W_n, Inf, X, Y, Z \rangle$$

де Θ_{BD} – множина троянських програм класу Trojan-Backdoor; $A_{\Theta_{BD}} = A'_{\Theta_{BD}} \cup A''_{\Theta_{BD}}$ – дії ТП, $A'_{\Theta_{BD}}$ – дії ТП, при потраплянні якої відбувається створення нового файлу, $A''_{\Theta_{BD}}$ – дії ТП, при потраплянні якої відбувається підміна системних файлів ТП; $W_n \in W$ – множини відправлених з КС файлів, шляхом виконання дій $a \in A$, що утворює множину ознак невірного функціонування структурних одиниць ОС КС $b_{BDi} \in B_{BD}$, $B_{BD} = \{b_{BD1}, b_{BD2}, ..., b_{BDn}\}$; Inf – ознака інфікування КС; X – відношення, що описує виконання ТП $n \in \Theta$ дій $a \in A$, $(n, a) \in X$, де $X \subset \Theta \times A$; Y – відношення дій ТП $a \in A$ та структурних одиниць ОС $(a, b) \in Y$, де $Y \subset A \times B$; Z – відношенням дій ТП $a \in A$ та файлів $w \in W$, $(a, w) \in Z$, де $Z \subset A \times W$.

Модель процесу діагностування комп'ютерних систем на наявність троянських програм

Було побудовано модель процесу ДТП КС на наявність ТП [3]:

$$M_u = \langle E, S, R, V, L, H, S, D, e, f \rangle,$$

де E – множина об'єктів діагностування $e_k \in E$; S – множина станів $s \in S$ об'єкту діагностування, які відповідають життєвому циклу ТП; V – матриця відношень дій $m \in M$ програмного об'єкту і системних портів КС $p \in P$; L – матриця відношень дій програмного об'єкту $a \in A$ та системних бібліотек КС $b \in B$; R – результуюче число $R \in [0,1]$, яке свідчить про ступінь небезпеки інфікування КС ТП; H – множина об'єктів $h \in H$, що підлягають процедурі сканування на предмет можливого факту їх підміни; S – множина бінарних послідовностей, згенерованих для формування набору захищених бінарних послідовностей $s \in S$; D – множина детекторів, згенерованих для сканування системи $d \in D$; e – відношення між об'єктами та станами, при чому для $n \in \Theta$ та $s \in S$, відношення $n\, e\, s$ означає, що програмний об'єкт e перебуває в стані s, відношення $e\, \bar{e}\, s$ означає, що програмний e не перебуває в стані s; $f_m(I_m, I'_m, I''_m)$ – функція адаптивності діагностування КС в режимі монітора, де I_m – набір діагностичної інформації, $I_m = \langle \Theta, V, L, R, \rangle$); I'_m – вектор результатів антивірусного діагностування, $I'_m = \langle R_1, R_2, ..., R_n \rangle$; I''_m – набір даних, які збираються про виявлене шкідливе програмне забезпечення і використовуються в майбутньому як знання, $I''_m = \langle E, R \rangle$; $f_s(I_s, I'_s, I''_s)$ – функція адаптивності діагностування КС в режимі сканера, $I_s = \langle H, S, D \rangle$ – набір діагностичної інформації; $I'_s = \langle E_1, E_2, ..., E_n \rangle$ – результат антивірусного сканування; $I''_s = \langle E'_1, E'_2, ..., E'_n \rangle$ – вектор інформації про оновлення та встановлення нового ПЗ.

Рис. 3. Достовірність діагностування КС на наявність нових троянських програм

Процес діагностування КС на наявність ТП представимо схемою, наданою на рис. 3:

Метод діагностування КС на наявність ТП в режимі монітора

Схема процесу діагностування КС на наявність ТП в режимі монітора представлена на рис. 4.

В основі ДТП в режимі монітора лежить використання механізму нечіткого логічного висновку (НЛВ) [4], для якого необхідна побудова вхідної та вихідної лінгвістичних змінних. Так ім'я для вхідної лінгвістичної змінної задамо «Ступінь підозрілості» програмного об'єкта, а ім'я для вихідної лінгвістичної змінної – «Ступінь небезпеки інфікування». Проте при формуванні функцій належності для вхідної лінгвістичної змінної виникають проблеми, оскільки поведінка ТП на етапах ЖЦ багатоваріантна, має нечіткий характер, не може бути прогнозованою, а їхні функції належності невизначені. Тому в роботі функції належності вхідної лінгвістичної змінної визначаються непрямим методом із залученням оцінок експертів. З цією метою виконуємо наступні кроки:

Рис. 4. Діагностування КС на наявність ТП в режимі монітора

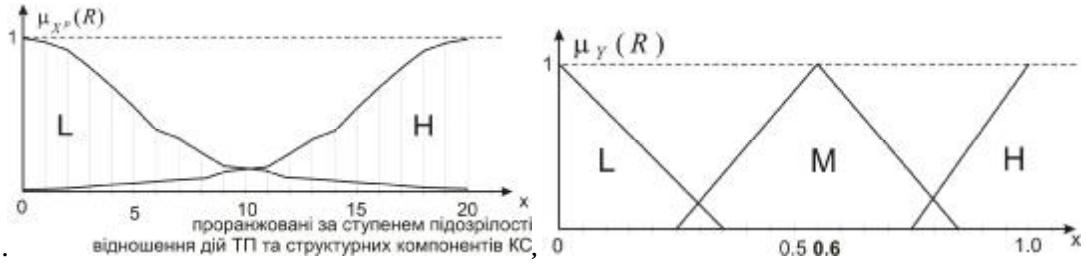
1) Знаходимо для кожної дії найбільш імовірний порт потрапляння шляхом ранжування, у якому попарне порівняння експерта виконується з урахуванням оціночних ознак, що дозволяють врахувати особливості порівнюваних об'єктів. З цією метою будуємо матрицю переваги $S = |s_{ij}|$, елементи якої визначаються обчисленням значень парних переваг по кожній ознаці окремо з урахуванням їх ваг з використанням формули:

$$s_{ij} = \frac{\sum_{k=1}^{r} s_{ij}^k \cdot p_k}{\sum_{k=1}^{r} s_{jk}^k \cdot p_k}; \; s_{ji} = \frac{1}{s_{ij}}; \; s_{ii} = 1; \; i, j = \overline{1, m}, \; s_{ij} = s_i / s_j, \; 0 < s_{ij} < \infty. \qquad (1)$$

2) Знаходимо для S власний вектор $\Pi = (p_1, ..., p_m)$, що відповідає максимальному додатному кореню l характеристичного полінома $|S - l \cdot E| = 0$; $S \cdot \Pi = l \cdot \Pi$, де E – одинична матриця. Компоненти вектора П ($\sum p_i = 1$) ототожнюються з оцінкою значення функції належності $m_{X^p}(x_i, y_j)$, що враховує прийняті деструктивні ознаки програмного об'єкта.

3) Будуємо матрицю $V_p = |x_i, y_j|$, у якій кожному відношенню (x_i, y_j) відповідає значення $0 \le p \le 1$, побудова оптимізованої матриці $V_p^* = |x_i, y_j|$, з відношень (x_i, y_j) (x_i, y_j) з найбільш вираженим деструктивним характером із значеннями $p_{\max}$ $(0 \le \pi_{\max} \le 1)$ та будуємо нормовану криву функції належності $m_{X^p}(R)$ вхідної змінної. Побудова функції належності $m_{X^a}(R)$ і $m_{X^e}(R)$ аналогічна.

Функції належності для вхідної та вихідної лінгвістичних змінних надано на рис. 5:



а) б)

Рис. 5. Функції належності лінгвістичних змінних: а) для вхідної, б) для вихідної

Була розроблена система нечіткого логічного висновку, графічне представлення якої надано на рис. 6.

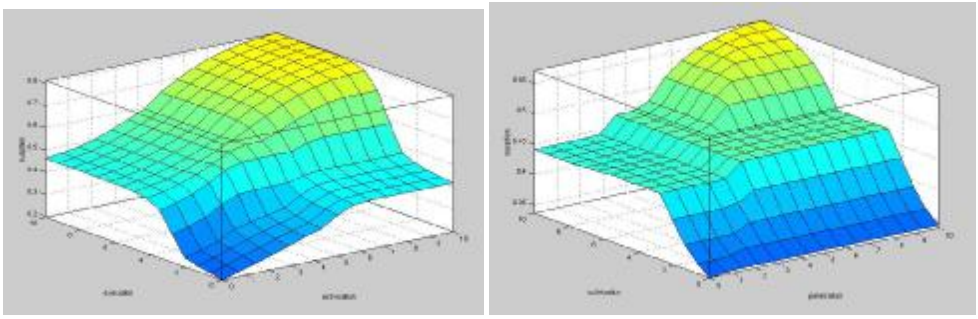


Рис. 6. Функції належності лінгвістичних змінних: а) для вхідної, б) для вихідної

Метод діагностування КС на наявність ТП в режимі сканера

Діагностування КС на наявність ТП в режимі сканера здійснюється із залученням апарату штучних імунних систем [5]. Метод включає кроки:

1) виконання формування набору системних файлів, що підлягають процедурі створення “свого” (системних бібліотек ОС, файлів системних служб та драйверів пристроїв), які можна вважати еталонними;

2) виконання кодування даних “свого” та “чужого” у вигляді визначеної послідовності згідно з типом ОС;

3) виконання генерації детекторів ТП в ПК одним із алгоритмів штучних імунних систем;

4) на етапі сканування системи виконання співставлення захищених послідовностей з детекторами. Висока афінність з детектором свідчить про виявлення аномалії в системі, що діагностується, та вимагає перевірки на підозрілість поведінки даного об’єкту.

Розв’язок задачі з використанням ШІС вимагає вирішення питання представлення даних «свого-чужого» – задачі кодування. Захищені послідовності кодуються шляхом визначення властивостей та параметрів файлів. Для операційної системи типу Linux, захищена послідовність має вигляд:

$$D_i^L = \left\langle m_1 \ldots m_i \ldots m_x, u_1 \ldots u_i \ldots u_x, g_1 \ldots g_i \ldots g_x, s_1 \ldots s_i \ldots s_x, t_1 \ldots t_i \ldots t_x, h_1 \ldots h_i \ldots h_y, C_1 \ldots C_i \ldots C_z \right\rangle,$$

де $m_1 \ldots m_i \ldots m_x$ – режим файлу (тип і права доступу); $u_1 \ldots u_i \ldots u_x$ – числовий ідентифікатор власника файлу, який показує власника файлу; $g_1 \ldots g_i \ldots g_x$ – числовий ідентифікатор групи власника файлу; $s_1 \ldots s_i \ldots s_x$ – розмір файлу; $t_1 \ldots t_i \ldots t_x$ – час останньої зміни файлу; $h_1 \ldots h_i \ldots h_y$ – створений хеш MD5 даного файлу; $C_1 .. C_i \ldots C_z$ – CRC даного файлу, при $i = \overline{1,n}$, де n – кількість детекторів.

Захищені послідовності для операційної системи типу Windows, має вигляд:

$$D_i^W = \left\langle s_1 \ldots s_i \ldots s_x, t_1 \ldots t_i \ldots t_x, a_1 \ldots a_i \ldots a_x, h_1 \ldots h_i \ldots h_y, C_1 \ldots C_i \ldots C_z \right\rangle,$$

де $s_1 \ldots s_i \ldots s_x$ – розмір файлу; $t_1 \ldots t_i \ldots t_x$ – час останньої зміни файлу; $a_1 \ldots a_i \ldots a_x$ – атрибут файлу (параметри: лише читання, прихований, системний архівний); $h_1 \ldots h_i \ldots h_y$ – створений хеш MD5 даного файлу; $C_1 .. C_i \ldots C_z$ – CRC даного файлу, при $i = \overline{1,n}$, де n – кількість детекторів.

Дослідження вибору оптимальних параметрів алгоритму негативного відбору було проведені роботі

[5] і показують ймовірність виявлення факту підміни файлів від 95 до 99 %.

Діагностування КС на наявність ТП в режимах монітора і сканера відбуваються за алгоритмами, описаними в [6].

Таким чином, розроблено адаптивну інформаційну технологію діагностування КС на наявність ТП, шляхом використання компонентів теорії штучного інтелекту, а саме апарату нечіткої логіки та штучних імунних систем, яка дозволяє здійснювати висновок щодо ступеня небезпеки інфікування КС троянською програмою як відомою, так і невідомою та виявляти факт підміни системних файлів троянськими версіями.

Адаптивна інформаційна технологія було реалізована у вигляді програмного забезпечення [7].

Результати достовірності діагностування КС на наявність ТП були отримані в результаті проведення експерименту, суть якого полягала в генерації програмних об'єктів з функційним навантаження класів троянських програм (таблиця 1). На згенерованому наборі програм були протестовані відомі засоби антивірусного діагностування КС на наявність ТП. Результаті показали достовірності діагностування до 74 %, що на 5-15 % вище у порівнянні з відомими засобами (рис. 7).

Таблиця 1

Результати діагностування КС на наявність троянських програм

Програмні об'єкти з властивостями ТП класу		Кількість програм, позначених як підозрілі	Відсоток виявлення, %
Rootkit	180	102	56,67
BackDoor	810	748	85,06
Trojan-PSW	320	251	78,44
Trojan-Clicker	210	82	66,19
Trojan Downloader	850	667	76,71
Trojan-Dropper	230	135	61,74
Trojan-Proxy	150	104	69,33
Trojan-Spy	330	235	71,21
Trojan-Notifier	160	86	63,13
Всього ТП	3240	2410	

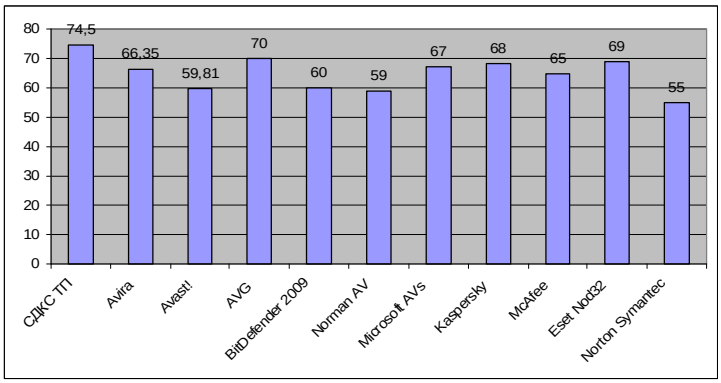


Рис. 7. Ефективність адаптивної інформаційної технології діагностування КС на наявність ТП

Висновки

Вперше одержано поведінкову модель троянських програм комп'ютерних систем та поведінкові моделі класів троянських програм, які враховують особливості їх функціонування та деструктивний характер дій в комп'ютерній системі. Розроблені множини поведінкових моделей троянських програм дозволили побудувати модель процесу діагностування комп'ютерних систем на наявність троянських програм, яка відрізняється від відомих залученням компонентів штучного інтелекту, зокрема нечіткої логіки та алгоритмів штучних імунних систем, що надало процесу діагностування КС на наявність троянських програм адаптивної характеристики. Використання даної моделі робить можливим здійснення діагностування КС на наявність ТП за допомогою аналізу поведінки підозрілих програмних об'єктів в КС.

Розроблено метод діагностування комп'ютерних систем на наявність троянських програм для визначення ступеня небезпеки інфікування комп'ютерної системи троянськими програмами з використанням механізму нечіткого логічного висновку. Для задання лінгвістичної змінної у частині знаходження функцій належності виконується попарне порівняння експертом з урахуванням оціночних ознак, яке дозволяє врахувати особливості порівнюваних об'єктів, і яке не вимагає виконання умови транзитивності.

Розроблено метод діагностування комп'ютерних систем на наявність троянських програм для визначення факту підміни системних файлів троянськими версіями із застосуванням алгоритмів штучних імунних систем.

Розроблено адаптивну інформаційну технологію діагностування комп'ютерних систем на наявність ТП, суть якої полягає у використанні розроблених поведінкових моделей класів троянських програм, відмінністю якої від відомих є те, що процес діагностування не потребує побудови баз сигнатур, дає змогу

виявляти нові невідомі троянські програми та підвищує достовірність і ефективність процесу діагностування комп'ютерних систем на наявність троянських програм.

Розроблено програмне забезпечення, яке дозволяє здійснювати антивірусні моніторинг та сканування, і задачею якого є діагностування КС на наявність як відомих, так невідомих троянських програм. Отримані результати діагностування КС на наявність ТП показали підвищення достовірності ТП до 74 %, що на 5-15 % вище у порівнянні з відомими засобами діагностування КС на наявність нових троянських програм.

Література

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

2. Савенко О.С. Процес виявлення троянських програм з використанням поведінкової моделі троянських програм на основі матриць відношень / О.С. Савенко, С.М. Лисенко // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2007. – № 1. – С. 69-74.

3. Савенко О.С. Модель процесу пошуку троянських програм в персональному комп'ютері / Олег Савенко, Сергій Лисенко // Радіоелектронні і комп'ютерні системи. – 2008. – № 7. – С. 87-92.

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

5. 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.

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

7. Лисенко С.М. Розробка програмного забезпечення реалізації інтелектуального методу пошуку троянських програм в персональних комп'ютерах / С.М. Лисенко, А.П. Гонтар, А.С. Шевцов // Вісник Хмельницького національного університету. – 2010. – № 1, Том 1. – С. 98-105.

Надійшла 16.5.2010 р.

УДК 004.492.3

М.Д. МАРКОВСЬКИЙ, О.В. ПОМОРОВА
Хмельницький національний університет

РОЗРОБКА МЕТОДУ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СЕРВІСІВ В ГЛОБАЛЬНИХ ТА ЛОКАЛЬНИХ МЕРЕЖАХ

В роботі проведено аналіз сучасного стану в галузі антивірусного програмного забезпечення, розроблено новий метод передачі оновлень баз антивірусів, що ґрунтується на зомбі мережі, яка поєднує в собі децентралізовану (P2P) та централізовану топологію.

In operation the analysis of a present status of the anti-virus software has been carried out. The new method of transmission of signatures of anti-virus basises which is grounded on the zombie network which joints in itself decentralised (P2P) and the centralised topology is developed.

Ключові слова: антивірус, p2p, бот, ботнет, передача даних, захист, безпека.

Комп'ютерні технології на сьогодні інтенсивно впроваджуються у різні галузі, зокрема банківські системи та комунікаційні системи, медичні комплекси, системи керування атомними станціями і т. і.

При цьому все більшої актуальності набуває стабільність та надійність функціонування програмного забезпечення (ПЗ). Наряду з корисним програмним ПЗ з'являються і програмні додатки руйнівної та дестабілізуючої дії, зокрема, таке шкідливе програмне забезпечення, як комп'ютерні віруси.

За статистикою, з кожним роком кількість шкідливого програмного забезпечення зростає. З 1992 року по 2007 рік було виявлено близько 2 млн унікальних шкідливих програм, а за період з 2007 до 2008 року – вже 15 мільйонів [1].

Збільшення кількості шкідливого програмного забезпечення призводить до зростання частоти знищення інформації, викрадення паролів та кодів, дестабілізації функціонування комп'ютерних систем (КС), що у результаті збільшує фінансові втрати користувачів. Неможливо в повному обсязі підрахувати світовий фінансовий збиток, що наноситься вірусами. За даними досліджень «Symantec», кожна велика корпорація щорічно втрачає близько 2 млн доларів в результаті кібератак.

З огляду на тенденції збільшення кількості вірусів та фінансових втрат в результаті їх дій актуальною є задача забезпечення захисту комп'ютерних систем. На підприємствах, зазвичай, усі або велика кількість КС об'єднані в мережу. Якщо хоча б один комп'ютер мережі заражений вірусом, то існує загроза зараження всієї мережі, що призводить до збільшення ризиків фінансових втрат.