УДК 004.492.3

С.М. ЛИСЕНКО
Хмельницький національний університет

ОЦІНКА ЕФЕКТИВНОСТІ ЗАСОБІВ АНТИВІРУСНОГО ДІАГНОСТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ

В роботі розроблено методику оцінки ефективності засобів антивірусного діагностування. До уваги взято такі показники, як достовірність роботи антивірусних монітора та сканера, тривалість діагностування та об'єми даних, що проходять в процесі антивірусного діагностування.

Ключові слова: антивірусне діагностування комп'ютерних систем, ефективність антивірусного діагностування, троянські програми, worm-віруси, ботнет, поліморфний код.

S. M. LYSENKO
Khmelnytskyi national university

EVALUATION OF THE ANTIVIRUS COMPUTER SYSTEMS DIAGNOSIS

Abstract. In order to estimate the efficiency of the antivirus diagnosis the new technique was developed. It takes into account the efficiency in the monitor and scanner modes, antivirus diagnosis duration for different modes and the data that are involved during the antivirus diagnosis. In the article the influence of operation system is researched.

Keywords: antivirus diagnosis, efficiency of antivirus diagnosis, Trojans, worm-viruses, botnet, polymorph code.

Вступ

Антивірусне програмне забезпечення – програмне забезпечення (ПЗ), призначене для виявлення комп'ютерних вірусів, а також програм, що вважаються шкідливими, для відновлення інфікованих (модифікованих) такими програмами файлів, а також для профілактики – запобігання зараженню (модифікації) файлів або операційної системи шкідливим кодом [1, 2].

На даний момент антивірусне програмне забезпечення розробляється, в основному, для операційних систем (ОС) сімейства Microsoft Windows ©, що пов'язано з великою популярністю та поширеністю даної ОС.

Роль антивірусного забезпечення сьогодні важко переоцінити, оскільки кількість шкідливого програмного забезпечення (ШПЗ) стрімко зростає [3]. Незважаючи на значну кількість антивірусного ПЗ, користувачам важко здійснити вибір, який однозначно задовольнить їх вимоги щодо антивірусного діагностування комп'ютерних систем [4, 5].

Постановка задачі

Таким чином, актуальною є задача розробки методики оцінювання ефективності антивірусного діагностування комп'ютерних систем з урахуванням параметрів антивірусного діагностування та ресурсів операційної системи, які використовує антивірусний засіб для діагностування.

Основний розділ

Ефективністю антивірусного діагностування комп'ютерних систем (ДКС) вважатимемо універсальну характеристику функціонування антивірусного засобу, що враховує результативність виявлення ШПЗ та ресурси, котрі залучаються в процесі антивірусного діагностування. Взаємодію антивірусного засобу з ШПЗ та з операційною системою представлено схемою на рисунку 1.

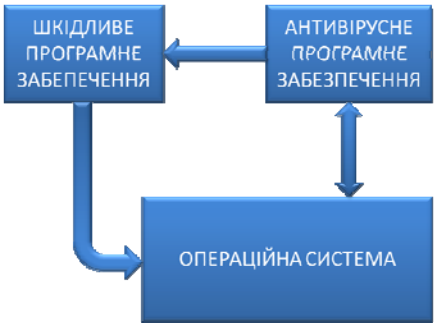

Рис. 1. Результати тестування АПЗ

Ефективність діагностування комп'ютерних систем (КС) на наявність шкідливого програмного забезпечення визначають антивірусні монітор та сканер, які взаємодіють з одного боку з ШПЗ та з операційною системою - з іншого.

Таким чином, загальна ефективність антивірусного діагностування КС враховує результати антивірусного діагностування та програмно-апаратні ресурси, які використовуються в процесі антивірусного діагностування, і визначається:

$$P = \frac{E}{R}, \qquad (1)$$

де E - ефективність роботи антивірусного засобу, яка включає достовірність роботи монітора та сканера; R - ресурси, що залучаються для здійснення антивірусного діагностування.

Монітор і сканер функціонують у двох режимах: автономному та оперативному. Показниками для режимів діагностування, які впливатимуть на ефективність роботи антивірусного засобу, є достовірність роботи монітора в оперативному режимі D_M та достовірність роботи сканера в оперативному режимі D_S. Таким чином, ефективність роботи антивірусного засобу $E = f(D_M, D_S)$ складе:

$$E = D_M + D_S. \qquad (2)$$

Ресурсами, що залучаються для здійснення антивірусного діагностування, вважатимемо тривалість ДКС на наявність ШПЗ в оперативному режимі сканера T_S; середню тривалість ДКС в оперативному режимі монітора T_M; середній час підготовки ДКС до експлуатації в автономному режимі сканера T_s^P; середній час підготовки ДКС до експлуатації в автономному режимі монітора $T_м^P$; об'єми даних, що проходять в процесі ДКС в режимі монітора V_M; об'єми даних, що проходять у в процесі ДКС в режимі сканера V_S. Ресурси, що залучаються для здійснення антивірусного діагностування $R = f(T_M, T_S, T_M^P, T_S^P, V_M, V_S)$, розраховуватимемо:

$$R = T_M \cdot V_M + T_S \cdot V_S + T_M^P \cdot V_м^P + T_S^P \cdot V_S^P, \tag{3}$$

Для оцінки ефективності антивірусного діагностування введемо показник хибних спрацювань ДКС на наявність ШПЗ в режимах монітора та сканера, який обчислимо за формулами:

$$X_M = \frac{\sum_{i=1}^{s} x_i}{X}, \qquad X_S = \frac{\sum_{i=1}^{s} x_i}{X}, \tag{4}$$

де X – загальна кількість програм, x_i – кількість програм, віднесених антивірусним засобом до *i*-го типу шкідливого програмного забезпечення.

В процесі роботи антивірусного засобу явище хибних спрацювань також використовує ресурси, що відображається зниженням рівня ефективності антивірусного діагностування $R_X = f(X_M, T_{X_M}, V_{X_M}, X_S, T_{X_S}, V_{X_S})$ на величину:

$$R_X = X_M \cdot T_{X_M} \cdot V_{X_M} + X_S \cdot T_{X_S} \cdot V_{X_S}, \tag{5}$$

де X_M, X_S - показники хибних спрацювань в режимах монітора сканера; T_{X_M}, T_{X_S} - показники часу, затраченого на хибні спрацювання в режимах монітора та сканера; V_{X_M}, V_{X_S} - об'єми даних, що проходять в процесі хибних спрацювань в режимах монітора та сканера.

Отже, визначення ефективності діагностування КС на наявність шкідливого програмного забезпечення з урахуванням показника хибних спрацювань, складе:

$$P = \frac{E}{R + R_X}. \tag{6}$$

Достовірністю результатів роботи діагностування в оперативному режимі монітора вважатимемо значення відношення виявленого ШПЗ до усієї кількості ШПЗ . Приймемо n_i, $i = \overline{1,s}$, $s \in N$ як кількість ШПЗ *i*-го типу, k_i – кількість об’єктів ШПЗ, виявлених антивірусним засобом. Тоді достовірність результатів роботи діагностування в оперативному режимі монітора D_M складе:

$$D_M = \frac{\sum_{i=1}^{s} \alpha_i \cdot k_i}{\sum_{i=1}^{s} \alpha_i \cdot n_i}, \tag{7}$$

де α_i – відсоток і-го класу від усього ШПЗ, $0 \le \alpha_i \le 1$.

Обчислення достовірності результатів роботи засобів антивірусного діагностування КС в оперативному режимі сканера D_S здійснимо за формулою (7).

Середній час підготовки ДКС на наявність ШПЗ до експлуатації в автономному режимі сканера T_s^P залежить від часу здійснення оновлень баз та модулів антивірусного засобу, а тривалість ДКС на наявність ШПЗ в оперативному режимі сканера T_S залежить від часу, що затрачається на пошук сигнатури або часу евристичного виявлення ШПЗ.

Під тривалістю ДКС на наявність ШПЗ в оперативному режимі монітора T_M розглядатимемо час t_b здійснення пошуку b_j -ї сигнатури або поведінки в базі, а середній час підготовки ДКС на наявність ШПЗ до експлуатації в автономному режимі монітора $T_м^P$:

$$T_M = \sum_{j=1}^{v} t_b, \qquad T_м^P = \sum_{l=1}^{r} t_p, \tag{8}$$

де t_p – час , необхідний для занесення $l = \overline{1,r}$ сигнатур та поведінок ШПЗ до бази.

Об'єми даних $V_{Mt_{умм}}$, що проходять в процесі ДКС на наявність ШПЗ в режимі монітора за одну умовну одиницю часу, визначимо як суму об’ємів даних, помножених на частоту запитів даних на одну умовну одиницю часу n_r:

$$V_{Mt_{умм}} = V_M^s \cdot n_r^s + V_M^p \cdot n_r^p + V_M^a \cdot n_r^a + V_M^e \cdot n_r^e + V_M^f \cdot n_r^f, \tag{9}$$

де V_M^s - об'єм даних, що проходить при ДКС при здійсненні відслідковування системних подій; V_M^p, V_M^a, V_M^e - об'єм даних, що використовується при пошуку необхідної сигнатури або поведінки ШПЗ на етапах потрапляння, активізації, виконання функцій; V_M^f – об'єм даних, що використовується при здійсненні НЛВ. Тоді з урахуванням часу необхідного для реалізації кожного етапу загальний об'єм даних, що проходять в процесі ДКС в режимі монітора V_M обчислимо так:

$$V_M = V_{Mt_{ум}} \cdot n_{t_{ум}}. \quad (10)$$

Об'єми даних, що проходять у ДКС на наявність ШПЗ в процесі діагностування КС на наявність ШПЗ в режимі сканера $V_{St_{ум}}$ за одну умовну одиницю часу, визначимо аналогічно (10):

$$V_{St_{ум}} = V_S^p \cdot n_r^p + V_S^d \cdot n_r^d + V_S^h \cdot n_r^h + V_S^u \cdot n_r^u, \quad (11)$$

де V_S^p – об'єм даних, що проходить при ДКС при здійсненні налаштування параметрів сканування; V_S^d – об'єм даних, що проходить в процесі ДКС при здійсненні порівняння сигнатури ПЗ та сигнатури з бази ШПЗ; V_S^h – об'єм даних довідки; V_S^u – об'єм даних оновлень. Тоді з урахуванням часу необхідного для реалізації кожного етапу загальний об'єм даних, що проходять у процесі ДКС в режимі сканера V_M, обчислимо:

$$V_S = V_{St_{ум}} \cdot n_{t_{ум}}. \quad (12)$$

Для визначення загальної ефективності ДКС на наявність ШПЗ використаємо показники ДКС на наявність ШПЗ, що визначають експлуатаційну ефективність ДКС:

а) ефективність роботи антивірусного засобу E, що визначається на основі максимізації значення достовірності діагностування КС на наявність ШПЗ в оперативному режимі монітора $D_M \to \max$ та максимізації значення достовірності діагностування КС на наявність ШПЗ в оперативному режимі сканера $D_S \to \max$; цільове значення показника $E \to \max$;

b) ресурси, що залучаються для здійснення антивірусного діагностування, які визначаються на основі мінімізації значень середньої тривалість діагностування, середнього часу підготовки до діагностування та мінімізації об'ємів даних, що проходять в процесі ДКС в режимах монітора та сканера, $T_M \to \min$, $T_M^P \to \min$, $T_S \to \min$, $T_S^P \to \min$, $V_M \to \min$, $V_S \to \min$, а також мінімізації показників, що залучаються в процесі хибних спрацювань, $X_M \to \min, T_{X_M} \to \min, V_{X_M} \to \min, X_S \to \min, T_{X_S} \to \min, V_{X_S} \to \min$.

Дослідження характеристик та показників системи діагностування дають можливість здійснити визначення достовірності та ефективності антивірусного діагностування КС на наявність ШПЗ.

Експерименти та дослідження

Експерименти проводилися для ОС сімейства Windows. Для дослідження ефективності антивірусних засобів було здійснено оцінку для найбільш поширених антивірусних засобів. Експеримент проводився шляхом запуску 55 вірусних програм, що відносяться до різних класів ШПЗ [6–8], співвідношення яких подано в таблиці 1.

Таблиця 1

Співвідношення ШПЗ, яке було використано для проведення експериментів

Клас ШПЗ	Кількість
Троянські програми	15
Worm-віруси	14
Ботнет	14
Поліморфний код	6
Рекламне ШПЗ	6

Примітка. Вказаний набір ШПЗ за своїм функційним навантаженням не впливав на роботу системного реєстру операційних систем та антивірусних засобів, що дало змогу проводити експеримент шляхом паралельного (одночасного) запуску ШПЗ в КС.

Експеримент проводився протягом 8 годин для врахування можливих оновлень антивірусних баз. Для реалізації експерименту було залучено 21 комп'ютерну систему: три типи операційних систем - Microsoft Windows XP ®, Microsoft Windows Vista ® та Microsoft Windows 7® з сімома антивірусними засобами.

Показники хибних спрацювань під час антивірусного діагностування в режимах монітора та сканера для різних операційних систем подано в таблиці 2. Результати експериментів для КС для різних операційних систем подано в таблицях 3–5 та рисунках 2–4.

Таблиця 2

Показники хибних спрацювань під час антивірусного діагностування

Засіб антивірусного діагностування	Показник ресурсів, використаних в процесі хибних спрацювань під час антивірусного діагностування для операційних систем, %		
	Windows XP	Windows Vista	Windows 7
Avira	3	3	3
Avast!	4	4	4
Microsoft AVs	5	4	4
Kaspersky	5	4	4
Zillia	2	4	3
Eset Nod32	5	4	3
Dr. Web	3	3	3

Таблиця 3

Результати експериментів для КС з операційною системою Microsoft Windows XP ®

Засіб антивірусного діагностування	достовірність роботи монітора в оперативному режимі,%	достовірність роботи сканера в оперативному режимі, %	тривалість ДКС на наявність ШПЗ в оперативному режимі сканера, хв	середня тривалість ДКС в оперативному режимі монітора, с	середній час підготовки ДКС до експлуатації в автономному режимі сканера, хв	середній час підготовки ДКС до експлуатації в автономному режимі монітора, с	об'єми даних, що проходять в процесі ДКС в режимі монітора, Mb	об'єми даних, що проходять у в процесі ДКС в режимі сканера, Mb	ефективності ДКС на наявність ШПЗ
Avira	95	99	23	4	5	29	532	3401	1.19
Avast!	93	98	35	3	3	33	532	3401	1.61
Microsoft AVs	88	98	31	1	1	52	532	3401	4.61
Kaspersky	93	96	18	1	1	100	532	3401	4.69
Zillia	86	86	25	1	1	53	532	3401	4.33
Eset Nod32	95	98	22	1	2	54	532	3401	4.23
Dr. Web	88	95	39	1	3	88	532	3401	3.62

Таблиця 4.

Результати експериментів для КС з операційною системою Microsoft Windows Vista ®

Засіб антивірусного діагностування	достовірність роботи монітора в оперативному режимі,%	достовірність роботи сканера в оперативному режимі, %	тривалість ДКС на наявність ШПЗ в оперативному режимі сканера, хв	середня тривалість ДКС в оперативному режимі монітора, с	середній час підготовки ДКС до експлуатації в автономному режимі сканера, хв	середній час підготовки ДКС до експлуатації в автономному режимі монітора, с	об'єми даних, що проходять в процесі ДКС в режимі монітора, Mb	об'єми даних, що проходять у в процесі ДКС в режимі сканера, Mb	ефективності ДКС на наявність ШПЗ
Avira	95	99	19	4	5	35	945	5573	0.72
Avast!	93	98	38	3	3	31	945	5573	0.97
Microsoft AVs	88	98	36	1	3	55	945	5573	2.19
Kaspersky	94	96	21	2	1	67	945	5573	1.56
Zillia	86	86	29	1	2	48	945	5573	2.28
Eset Nod32	95	98	27	1	2	47	945	5573	2.56
Dr. Web	88	95	38	1	2	76	945	5573	2.43

Таблиця 5

Результати експериментів для КС з операційною системою Microsoft Windows 7 ®

Засіб антивірусного діагностування	достовірність роботи монітора в оперативному режимі, %	достовірність роботи сканера в оперативному режимі, %	тривалість ДКС на наявність ШПЗ в оперативному режимі сканера, хв	середня тривалість ДКС в оперативному режимі монітора, с	середній час підготовки ДКС до експлуатації в автономному режимі сканера, хв	середній час підготовки ДКС до експлуатації в автономному режимі монітора, с	об'єми даних, що проходять в процесі ДКС в режимі монітора, Mb	об'єми даних, що проходять у в процесі ДКС в режимі сканера, Mb	ефективності ДКС на наявність ШПЗ
Avira	95	99	27	1	5	43	2322	13401	0.77
Avast!	93	98	32	1	3	38	2322	13401	0.93
Microsoft AVs	88	98	25	3	1	50	2322	13401	0.44
Kaspersky	93	96	25	1	2	98	2322	13401	1.04
Zillia	86	87	28	2	1	41	2322	13401	0.59
Eset Nod32	95	98	22	1	4	55	2322	13401	0.85
Dr. Web	88	94	36	1	3	81	2322	13401	0.89

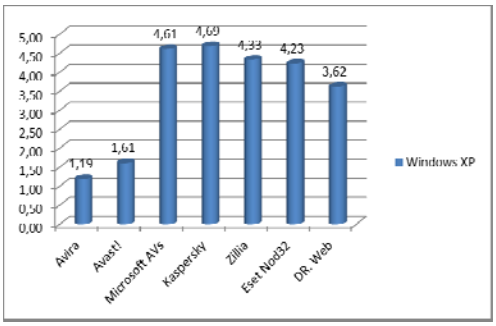

Рис. 2. Результати ефективності ДКС на наявність ШПЗ згідно з запропонованою методикою (Windows XP)

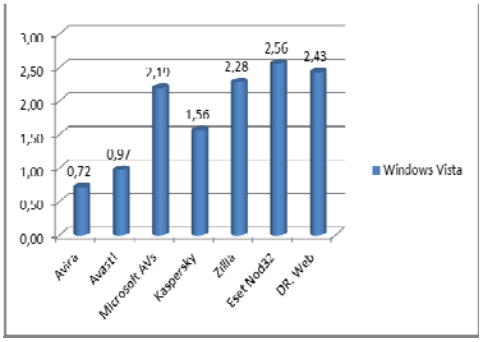

Рис. 3. Результати ефективності ДКС на наявність ШПЗ згідно з запропонованою методикою (Windows Vista)

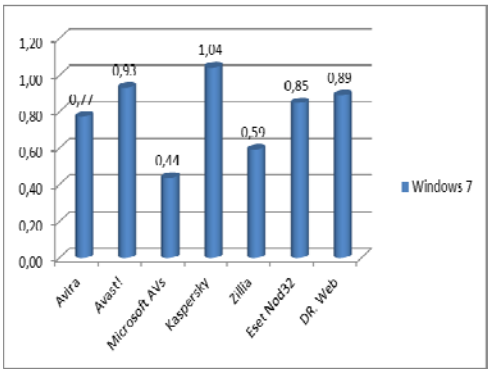

Рис. 4. Результати ефективності ДКС на наявність ШПЗ згідно з запропонованою методикою (Windows 7)

Висновки

Запропоновано методику визначення ефективності антивірусного діагностування комп'ютерних систем на наявність шкідливого програмного забезпечення. Розглянуто показники для режимів

діагностування, які впливають на ефективність антивірусного діагностування, а саме: достовірність роботи в режимах монітора та сканера, тривалість діагностування та об'єми даних, що проходять в процесі антивірусного діагностування.

В результаті дослідження експериментально з'ясовано, що достовірність роботи монітора та сканера для різних операційних систем та діагностування можуть відрізнятися. Також результати експериментів свідчать про приріст ефективності антивірусного діагностування у 20% для платформи Windows 7 та 14% для платформи Windows Vista у порівнянні з Windows XP, при цьому відмічається збільшення ресурсів, що використовуються в процесі діагностування для ОС Windows та Windows Vista.

Література

1. Tim Rains Operating System Infection Rates: Application Vulnerabilities & Exploits Trend Up, Increase OS Infection Rates [Електронний ресурс] - Режим доступу : http://blogs.technet.com/ b/security/ archive/ 2012/12/ 31/operating-system-infection-rates-vulnerabilities-amp-exploits-trending-up-increase-os-infection-rates.aspxt.

2. Williamson M. M. Virus throttling / M. M. Williamson, J. Twycross, J. Griffin // Virus Bulletin. – 2009.

3. VB100 Results Summary [Електронний ресурс] : Anti-Virus comparative. – http://www.virusbtn.com/vb100/archive/summary.

4. AV Comparatives laboratories [Електронний ресурс] – Access mode http://www.av-comparatives.org. – назва домашньої сторінки Інтернету.

5. Proactive/Retrospective test. [Електронний ресурс] : Anti-Virus comparative. – Режим доступу : http://av-comparatives.org. – назва домашньої сторінки Інтернету.

6. Savenko O. The Technique for Computer Systems Trojan Diagnosis in the Monitor Mode / Savenko O., Lysenko S. // Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications - USA, NJ 08855-1331: IEEE Operations Center, 2011 - vol.2, pp. 845-853.

7. Savenko O. Multi-agent based approach of botnet detection in computer systems / Savenko O., Lysenko S., Kryschuk A. // Computer Networks Communications in Computer and Information Science, 2012, Volume 291, pp. 171–180.

8. Гошко С.В. Энциклопедия по защите от вирусов / Гошко С.В. – М. : СОЛОН-Пресс, 2005. – 352 с.

References

1. Tim Rains “Operating System Infection Rates: Application Vulnerabilities & Exploits Trend Up, Increase OS Infection Rate” http://blogs.technet.com/ b/security/ archive/ 2012/12/ 31/operating-system-infection-rates-vulnerabilities-amp-exploits-trending-up-increase-os-infection-rates.aspxt.

2. Williamson M. M. TwycrossJ. Griffin, J. and Norman A. “Virus throttling”, Virus Bulletin, 2009.

3. “VB100 Results Summary”. Anti-Virus comparative http://www.virusbtn.com/vb100/archive/summary.

4. AV Comparatives laboratories http://www.av-comparatives.org.

5. Proactive/Retrospective test. Anti-Virus comparative. http://av-comparatives.org.

6. Savenko O., Lysenko S. “The Technique for Computer Systems Trojan Diagnosis in the Monitor Mode,” Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications - USA, NJ 08855-1331: IEEE Operations Center, 2011 - vol.2, pp. 845-853.

7. Savenko O., Lysenko S., Kryschuk A “Multi-agent based approach of botnet detection in computer systems,” Computer Networks Communications in Computer and Information Science, Vol. 291, 2012, pp. 171-180.

8. Goshko S. Encyclopedia of protection against viruses SOLON-Pres, 2005. (in Russian)

Рецензія/Peer review : 25.3.2013 р. Надрукована/Printed :7.4.2013 р.
Рецензент: д.т.н., проф. Поморова О.В.