УДК 004.056.53

Кассем Халіфе[1], Г.Я. Криховецький[2], Г.А. Кучук[1]

[1] *Національний технічний університет «Харківський політехнічний інститут», Харків*
[2] *Інститут спеціального зв'язку та захисту інформації НТУ України "Київський політехнічний інститут імені Ігоря Сікорського", Київ*

ОЦІНКА ВРАЗЛИВОСТІ СИСТЕМНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

У статті запропонована методика оцінки вразливості системного програмного забезпечення. Теоретична частина методики базується на методі динаміки середніх. Відмінною особливістю розробленої методики є врахування можливості масштабування процесу розробки програмного забезпечення шляхом впровадження фахівців з безпеки (PersonNon, SecDev) без суттєвої зміни ефективності розробки. На прикладі стратегії, прийнятої при імітаційному моделюванні, проведено дослідження і доведена доцільність використання додаткових фахівців з безпеки.

Ключові слова: *системне програмне забезпечення, безпека, вразливість, кібербезпека.*

Вступ

Постановка завдання. Проведені дослідження показали, що в даний час існують об'єктивні причини появи вразливостей в системному програмному забезпеченні (СПЗ), які полягають в надзвичайно високій структурній складності програмного коду, динамічності розвитку версій і відносній легкості модифікації коду [7 – 10]. До цього можна додати ряд проблем, пов'язаних з недосконалістю політик безпеки програмного забезпечення і недоліками тестування безпеки.

Дані фактори негативно впливають на процеси життєвого циклу програмного забезпечення і призводять до збільшення кількості успішно проведених кібератак на комп'ютерні системи в цілому.

Одним з актуальних питань, пов'язаних із захистом СПЗ, залишається оцінка його уразливості.

Аналіз літератури [1 – 10] показав, що, незважаючи на представлені теоретичні пропозиції, так і не забезпечено розробку математичного апарату для оцінки ступеня уразливості і безпеки програмного забезпечення. При цьому ряд експертів висуває припущення про неможливість визначення точних кількісних даних уразливості і безпеки СПЗ.

Тому широкого поширення набули методи якісної оцінки (наближені методи) оцінки вразливості СПЗ. Однак точність і адекватність такої оцінки залежить від ряду суб'єктивних факторів і з огляду на множину існуючих невизначеностей вхідних даних залишається низькою.

Мета статті. Розробити методику кількісної оцінки вразливості СПЗ, засновану на методі динаміки середніх, що отримав теоретичне обгрунтування в роботах [5, 6].

Результати досліджень

Основні положення методу динаміки середніх лягли в основу розробленої імітаційної моделі (рис. 1).

Методика передбачає виконання таких кроків.

Крок 1. Аналіз ймовірних загроз системному програмному забезпеченні. Змістовна постановка задачі дослідження.

Крок 2. Розробка операційної схеми для дослідження динамічної системи «СПЗ – ЗЛОВМИСНИК».

Блок 3. Складання рівнянь для станів в диференціальній формі відповідно до методу динаміки середніх.

Крок 4. Завдання вихідних даних, початкових і додаткових умов для вирішення завдання.

Крок 5. Чисельне рішення задачі, фіксація і апроксимація результатів моделювання.

Крок 6. Обчислення показників ефективності методу розробки системного ПЗ.

Кількісно ефективність розробленого методу можна визначити за допомогою показника втрат ΔZ_i по кожному засобу z_i. Цей показник визначає величину відносного збитку, нанесеного засобу z_i в результаті злочинних атак на ПЗ. При цьому, відповідно до робот [8, 9], показник відносної шкоди може бути обчислений за формулою:

$$\Delta Z_i\left(t^*\right)=\frac{z_i\left(t_0\right)-z_i\left(t^*\right)}{z_i\left(t_0\right)}\cdot 100\%,\quad i=1\ldots n, \quad (1)$$

де t* - поточний момент часу (момент виходу з циклу моделювання процесу); $\Delta Z_i\left(t^*\right)$ - відносний збиток для засобу z_i на момент часу t*; $z_i\left(t_0\right)$ - вихідний потенціал засобу z_i в момент часу t_0; n - кількість фазових координат (розмірність вектора z) динамічної системи «СПЗ - ЗЛОВМИСНИК».

Крок 7. Аналіз та узагальнення результатів моделювання і підготовка рекомендацій щодо вибору структури методології розробки системного ПЗ і стратегії її використання в фірмах.

© Кассем Халіфе, Г.Я. Криховецький, Г.А. Кучук

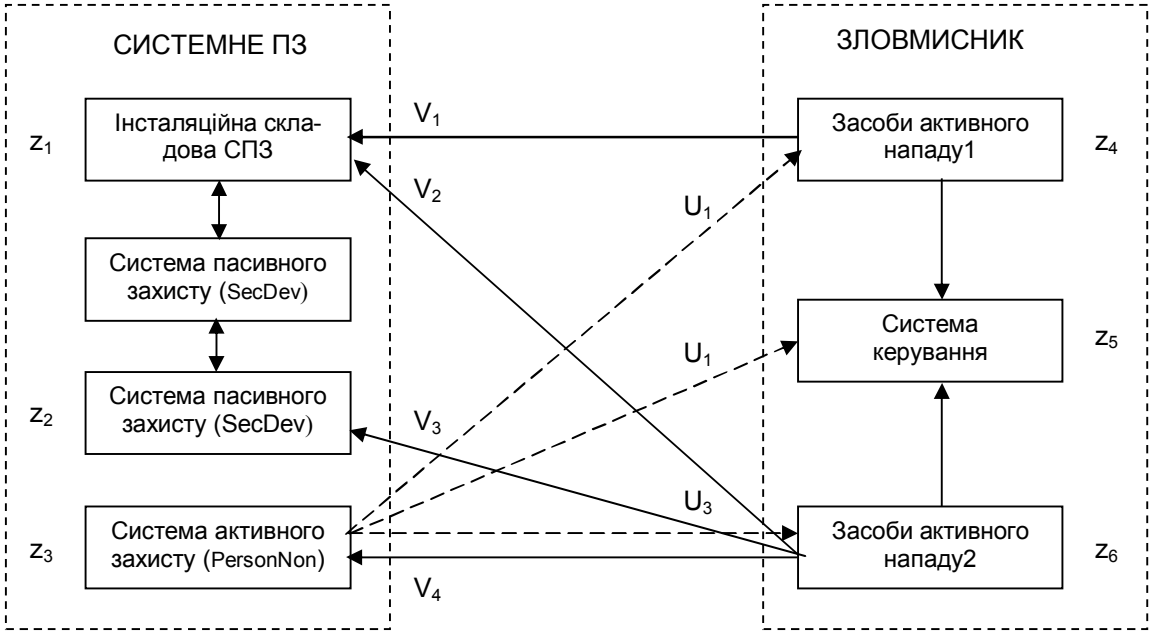


Рис. 1. Структура імітаційної моделі динамічної системи «СПЗ – ЗЛОВМИСНИК»

Обчислювальний експеримент з розробленою в середовищі MathCad програмою дозволяє для заданих умов реалізувати імітаційну модель процесу взаємодії системного ПЗ, як об'єкта нападу, і зловмисника та отримати оцінки показників ефективності використання розробленого методу. У представленій на рис. 1. моделі введемо допущення про використання засобів пасивного захисту для виявлення, локалізації та відновлення пошкоджених інформаційних та інших елементів системного ПЗ.

Для формалізованого представлення динамічної системи «СПЗ - ЗЛОВМИСНИК» введемо змінні z_i, $i=1\ldots6$, під якими будемо розуміти відповідно чисельності станів таких елементів: інсталяційних складових системного ПЗ, бази даних і засобів активного захисту ПЗ, засобів активного нападу першого типу, системи управління і засобів активного нападу другого типу зловмисника.

Стан динамічної системи «СПЗ - ЗЛОВМИСНИК» в цілому в кожен момент часу $t\in[t_0,t_N]$ характеризується системою звичайних лінійних диференціальних рівнянь (2), в якій в якості змінних розглядаються чисельності станів z_i, $i=1\ldots6$, а $\delta z_1\gamma_1\left(z_1,Z_1^*\right)$ – введення додаткових ресурсів (спеціалістів) для підвищення безпеки z_1; $\delta z_2\gamma_2\left(z_2,Z_2^*\right)$ – введення додаткових ресурсів (фахівців) для підвищення безпеки z_2; Z_1^* и Z_2^* – порогові значення чисельностей станів z_1 и z_2 відповідно, починаючи з яких вводиться резерв зі складу системи пасивного захисту; δz_1 и δz_2 – інтенсивності введення резервних засобів до складу z_1 и z_2;

$$\begin{cases}\dfrac{dz_1}{dt}=\bar{z}_1(t)=-\lambda_4p_{14}v_1z_4-\lambda_6p_{16}v_2z_6+\\ \qquad+\delta z_1\gamma_1\left(z_1,Z_1^*\right);\\ \dfrac{dz_2}{dt}=\bar{z}_2(t)=-\lambda_6p_{26}v_3z_6+\delta z_2\gamma_2\left(z_2,Z_2^*\right);\\ \dfrac{dz_3}{dt}=\bar{z}_3(t)=-\lambda_6p_{36}v_4z_6;\\ \dfrac{dz_4}{dt}=\bar{z}_4(t)=-\lambda_3p_{43}u_1z_3;\\ \dfrac{dz_5}{dt}=\bar{z}_5(t)=-\lambda_3p_{53}u_2z_3;\\ \dfrac{dz_6}{dt}=\bar{z}_6(t)=-\lambda_3p_{63}u_3z_3,\end{cases}\qquad(2)$$

де $\gamma_1\left(z_1,Z_1^*\right)$ и $\gamma_2\left(z_2,Z_2^*\right)$ сигнальні функції, які визначаються за формулами:

$$\gamma_1\left(z_1,Z_1^*\right)=\begin{cases}1, & \text{если } z_1(t)\le Z_1^*;\\ 0, & \text{если } z_1(t)>Z_1^*.\end{cases}$$

$$\gamma_2\left(z_2,Z_2^*\right)=\begin{cases}1, & \text{если } z_2(t)\le Z_2^*;\\ 0, & \text{если } z_2(t)>Z_2^*.\end{cases}$$

Відповідно до правил рішення [5], введемо змінні A_k, $k=1\ldots8$, для позначення коефіцієнтів диференціальних рівнянь:

$$A_1=-\lambda_4p_{14}v_1;\ \ A_2=-\lambda_6p_{16}v_2;\ \ A_3=0;$$

$$A_4=-\lambda_6p_{26}v_3;\ \ A_5=-\lambda_6p_{36}v_4;\ \ A_6=-\lambda_3p_{43}u_1;$$

$$A_7=-\lambda_3p_{53}u_2;\ \ A_8=-\lambda_3p_{63}u_3,$$

де λ_i, $i=1\ldots6$ – інтенсивності атак, які виконуються засобами z_i, $i=1\ldots6$ відповідно; $p_{i,j}$ – ймовірність проникнення (злому) в системне ПЗ або окрему її складову (наприклад, базу даних) z_i в резуль-

таті атаки із боку засобу z_j; u_1, u_2 та u_3 – коефіцієнти, що характеризують ступінь використання тестувальників вразливостей СПЗ (Person Non); v_1, v_2 та v_3 – коефіцієнти, що характеризують зусилля зловмисників, що долають захист системного ПЗ;

Після перетворень системи (2) отримаємо:

$$\begin{cases} \overline{Z}_1(t) = A_1 z_4 + A_2 z_6 + \delta z_1 \gamma_1\left(z_1, Z_1^*\right); \\ \overline{Z}_2(t) = A_3 z_6 + \delta z_2 \gamma_2\left(z_2, Z_2^*\right); \\ \overline{Z}_3(t) = A_4 z_6; \\ \overline{Z}_4(t) = A_5 z_3; \\ \overline{Z}_5(t) = A_6 z_3; \\ \overline{Z}_6(t) = A_7 z_3, \end{cases} \quad (3)$$

де $\gamma_k(t)$ – сигнальна функція, що дозволяє обрати інтервал введення резерву $\Delta t_{доп}$ (фахівців кібербезпеки) для поповнення засобів $z_1(t)$ и $z_2(t)$.

Співвідношення $u_1 / u_2 / u_3 = a / b / c$ визначають стратегію розробників СПЗ в відбитті атак зловмисників: v_1 - частка (%) засобів z_4 з боку зловмисників, які беруть участь в інформаційному придушенні засобів z_1 розробника СПЗ, причому повинна виконуватися умова: $v_1 \le 1$; v_2, v_3, v_4 – частки (в %) засобів з боку зловмисників, які беруть участь в інформаційному придушенні засобів z_1, z_2 и z_3, сторони розробника СПЗ відповідно; при цьому повинна виконуватися умова: $v_2 + v_3 + v_4 \le 1$; p_{ij}, $i, j = \overline{1,6}$ – ймовірність виведення з ладу засоби i-го типу засобом j-го типу.

При імітаційному моделюванні необхідно ввести додаткові умови:

1. Фахівці кібербезпеки в стані z_1 використовуються при $z_1(t) \le 80\%\, z_1(t_0)$, в стані z_2 використовуються при $z_2(t) \le 90\%\, z_2(t_0)$.

2. Кожен з блоків z_i, $i = \overline{3,6}$, має тільки два стани: працездатний та непрацездатний.

3. Вхідні дані імітаційної моделі прийняті такі:

$$z_1(t_0) = z_2(t_0) = 100; \quad z_3(t_0) = z_5(t_0) = 100\%;$$
$$z_4(t_0) = z_6(t_0) = 50.$$
$$\lambda_3 = 0{,}12 \text{год}^{-1}; \ \lambda_4 = 0{,}15 \text{год}^{-1}; \ \lambda_6 = 0{,}21 \text{год}^{-1};$$
$$\delta z_1 = 0{,}25 \text{год}^{-1}; \delta z_2 = 0{,}15 \text{год}^{-1}.$$

4. З урахуванням проведених досліджень і експертних оцінок фахівців фірм-розробників СПЗ прийняті фіксовані стратегії $\{u\}$ та $\{v\}$ сторін СПЗ і ЗЛОВМИСНИК:

$$u_1 = u_2 = 0{,}3; \quad u_3 = 0{,}25;$$
$$v_1 = 0{,}5; \quad v_2 = 0{,}25; \quad v_3 = 0{,}35; \quad v_4 = 0{,}4.$$

Значення ймовірностей виведення з ладу однієї одиниці СПЗ або засобів зловмисників приймемо відповідно до даних табл. 1.

Таблиця 1

Значення ймовірностей виведення з ладу однієї одиниці СПЗ і засобів зловмисників

СПЗ				ЗЛОВМИСНИК		
p_{14}	p_{16}	p_{26}	p_{36}	p_{43}	p_{53}	p_{63}
0,1	0,08	0,09	0,03	0,08	0,125	0,06

5. Моделювання (чисельне рішення) диференціальних рівнянь (2) виконано в циклі на інтервалі часу від 0 до 180 годин із кроком 6 хвилин .

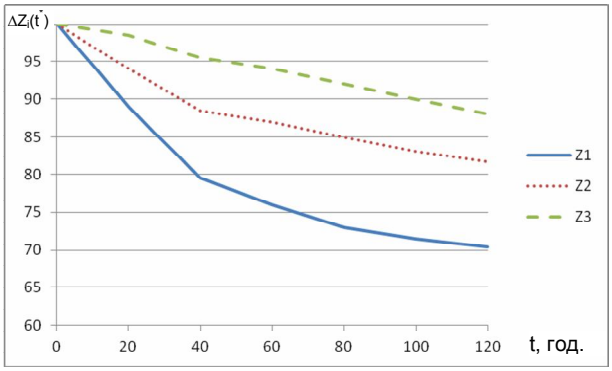
6. Обмеженнями моделювання, при яких неможливо продовження заданої програми є випадки коли $z_1 \le 1$; $z_2 \le 1$; $z_3 \le 10\%$; $z_4 \le 1$; $z_5 \le 10\%$; $z_6 \le 1$. Обчислимо відносний збиток $\Delta Z_i(t^*)$ для всіх z_i, де i = 1, ..., 6. Результати обчислень представлені в табл. 2.

Таблиця 2

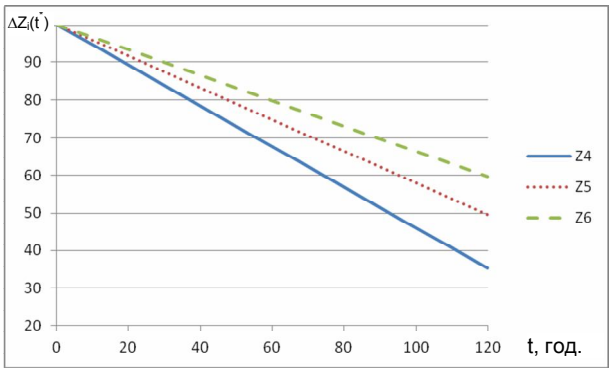
Відносний збиток $\Delta Z_i(t^*)$ для всіх z_i при t^*=120 годин

СПЗ			ЗЛОВМИСНИК		
$\Delta Z_1(t^*)$	$\Delta Z_2(t^*)$	$\Delta Z_3(t^*)$	$\Delta Z_4(t^*)$	$\Delta Z_5(t^*)$	$\Delta Z_6(t^*)$
29,57	18,31	11,99	64,57	50,45	40,36

Результати імітаційного моделювання, представлені у вигляді кривих на графіках рис. 2, дозволяють проаналізувати динаміку протистояння СПЗ-ЗЛОВМИСНИК.



а



б

Рис. 2. Динаміка змін $\Delta Z_i(t^*)$

У розглянутому прикладі результати імітаційного моделювання свідчать про доцільність та ефективність реалізованої в моделі системи захисту і, одночасно, про можливість нейтралізації засобів атакуючої сторони (використовуючи активні і пасивні методи захисту).

Оцінити ефективність розробленого методу можна по кривих графіків рис. 3.

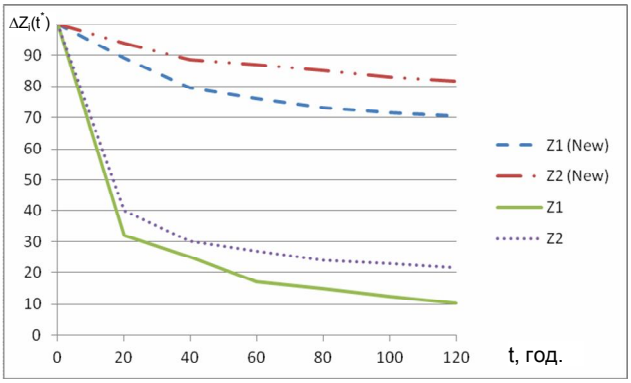


Рис. 3. Динаміка змін $\Delta Z_i(t^*)$ для систем із SecDev та Person Non, а також без них

Як видно з графіків рис. 1 – 3 використання розробленої методики масштабування процесу розробки СПЗ з урахуванням вимог безпеки знижує показник відносного збитку на всіх етапах життєвого циклу ПЗ до 6 разів, в залежності від можливої тривалості атаки.

Висновки

Таким чином, вдосконалена методика оцінки вразливості системного ПЗ. Її відмінною рисою є врахування можливості масштабування процесу розробки програмного забезпечення шляхом впровадження фахівців безпеки (PersonNon, SecDev). Це дозволить провести кількісну оцінку вразливості СПЗ з урахуванням існуючих вимог безпеки розробки програмного забезпечення. Надалі розроблена методика дозволить провести оцінку достовірності результатів імітаційного моделювання при аналізі методу масштабування процесу розробки програмного забезпечення.

Список літератури

1. ISO/IEC «Информационная технология Методы и средства обеспечения безопасности - Критерии оценки безопасности ИТ - Часть 1: Введение и общая модель». ISO/IEC JTC 1/SC27 №2738, 02.2001 г.

2. ISO/IEC 15408 3: 1999 «Информационная технология - Методы и средства обеспечения безопасности - Критерии оценки безопасности ИТ -Часть 3: Гарантийные требования безопасности».

3. ISO/IEC PDTR 15446 «Информационная технология Методы и средства обеспечения безопасности - Руководство по разработке профилей защиты и заданий по безопасности», ISO/IEC JTC 1/SC27 №2603 dra, 04.2001 г.

4. ISO 9001:1994 «Системы качества Модель для гарантии качества в проектировании, разработке, изготовлении, установки и обслуживании».

5. Надеждин Е.Н. Оценка эффективности механизма защиты сетевых ресурсов на основе игровой модели информационного противоборства. Научный вестник: ООО "Консалтинговая компания Юком" (Тамбов). № 2(4). С. 49-58. ISSN: 2411-1872.

6. Kuchuk, G., Kharchenko, V., Kovalenko, A. and Ruchkov E. (2016), "Approaches to Selection of Combinatorial Algorithm for Optimization in Network Traffic Control of Safety-Critical Systems", Proceedings of IEEE East-West Design & Test Symposium (EWDTS'2016), pp. 384–389.

7. Семенов С.Г., Кассем Халифе, Захарченко М.М. Усовершенствованный способ масштабирования гибкой методологии разработки программного обеспечения. Сучасні інформаційні системи. Харків :. НТУ «ХПІ». Т. 1, № 1. С. 19-24.

8. Frank Swiderski, Window Snyder "Threat Modeling", Microsoft Press 2004. ISBN 978-0-7356-1991-3.

9. Jean Francois Monin, Michal G. Hichey (editor) "Understanding Formal Methods", Springer-Verlag 2003, ISBN 1-85233-247-6.

10. Matt Bishop "Computer Security. Art and Science", Addison-Wesley 2003, ISBN 0-201-44099-7.

Надійшла до редколегії 1.11.2017

Рецензент: д-р техн. наук, проф. І.В. Рубан, Харківський національний університет радіоелектроніки, Харків.

ОЦЕНКА УЯЗВИМОСТИ СИСТЕМНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Кассем Халифе, Г.Я. Крыховецкий, Г.А. Кучук

В статье предложена методика оценки уязвимости системного программного обеспечения. Теоретическая часть методики базируется на методе динамики средних. Отличительной особенностью разработанной методики является учет возможности масштабирования процесса разработки программного обеспечения путем внедрения специалистов по безопасности (PersonNon, SecDev) без существенного изменения эффективности разработки. На примере стратегии, принятой при имитационном моделировании, проведено исследование и доказана целесообразность использования дополнительных специалистов по безопасности.

Ключевые слова: *системное программное обеспечение, безопасность, уязвимость, кибербезопасность.*

EVALUATION OF VULNERABILITY OF SYSTEM SOFTWARE

Kassem Khalife, H.Ya. Krikhovetskiy, H.A. Kuchuk

The article suggests a methodology for assessing the vulnerability of system software. The theoretical part of the methodology is based on the method of the dynamics of averages. A distinctive feature of the developed methodology is the possibility of scaling the software development process by implementing security experts (PersonNon, SecDev) without significantly changing the development efficiency. On the example of the strategy adopted in the simulation simulation, a study was conducted and the expediency of using additional security specialists was proved.

Keywords: *system software, security, vulnerability, cybersecurity.*