УДК 004.621.3

Скачек Л.М.
(ДУІКТ)

ЕФЕКТИВНІСТЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Вступ

Поняття "ефективність" не має єдиного загального визначення, та, за правило, інтерпретується за допомогою інших понять, пов'язаних з методами, отриманими числовими вимірюваннями й заснованими для них оцінками. Це пояснюється багатозначністю англомовних інтерпретацій латинського слова effectus (дія): effectiveness – досягнення мети незалежно від витрат; effecxiciency – оптимізація співвідношення "витрати-результати", незалежно від досягненні мети; effectuality – поєднання effectiveness і efficiency [1, 2, 3]. Враховуючи те, що у всіх приведених інтерпретаціях ефективності явно фігурують "мета" та "витрати", числова оцінка ефективності повинна описуватися не абсолютними, а порівняльними значеннями співвідношення ступеня досягнення мети й витрачених ресурсів [1, 3].

В зв'язку з цим, для використання формальних методів розрахунку оцінок ефективності, це поняття доцільно співвіднести з поняттям "оптимальність" інформаційного забезпечення, числова оцінка ефективності повинна описуватися не абсолютними, а порівняльними значеннями, співвідношенням ступеня досягнення мети і витрачених ресурсів, тобто, знаходження умов задоволення заданим критеріям (ціль, результати) при заданих обмеженнях змінних, які входять до критеріїв (затрати, ресурси). В цих термінах та визначеннях "підвищення ефективності " означає зниження витрат (використання ресурсів), шляхом систематичного приближення до встановленої цілі [98].

Моделі оцінки ефективності вперше розроблялися для використання в економіці, наприклад, для опису темпів фінансової віддачі від інвестицій за відносною оцінкою "ефективність-вартість (cost-effectiveness modeling)", при цьому, під "оптимізацією ефективності" розуміють максимізацію прибутку на одиницю інвестицій [3].

На відміну від економіки, задача оцінки ефективності безпеки інформаційної системи (ІС) на підприємстві, стала розвиватися тільки останнім часом (information systems effektiveness), що пов'язано з необхідністю мінімізації реакції ІС (response time) при максимізації релевантності виданих відповідей [4].

З розгляду поняття "ефективність" надамо всі наші подальші міркування щодо удосконалення умов підвищення організаційно-економічної ефективності безпеки підприємства.

Реакція ІС на підприємстві зв'язується з швидкодією програмно-технічного забезпечення (ПТЗ) (числом операцій в секунду) або складнішим поняттям "продуктивність " (performance), при цьому оптимізація реакції ІС в основному оцінюється технологічними затримки обробки запиту (delay) – швидкість роботи процесора, серверів, швидкість в каналах, час звернення до дискового простору та пристроїв зберігання, швидкість введення-виводу [6-9].

Слід також враховувати, що в мультипроцесорних (конвеєрних) та мультипрограмних ІС під час очікування операцій введення/вивід або при розпаралелюванні роботи програми, процесори можуть виконувати інші програми, тому ІС не обов'язково мінімізуватиме час виконання даної програми, а загальна оцінка ефективності інформаційної безпеки на підприємстві ускладнюється [10].

Мета роботи - проілюструвати новий підхід щодо удосконалення умов підвищення організаційно-економічної ефективності безпеки підприємства, яка пов'язана з швидкодією програмно-технічного забезпечення (ПТЗ) або складнішим поняттям "продуктивність ".

Результати досліджень

Найпоширенішим методом оцінки ефективності безпеки інформації на підприємстві є оцінка загальної ефективності устаткування (Overall Equipment Effectiveness, *OEE*), перенесена в область ІБ із області складних промислових багаторівневих конвеєрних систем [1, 5].

Обчислення оцінки P за методом *OEE* засновано на перемножуванні трьох параметрів: A – працездатності (availability), P – продуктивності (performance), і Q – якості (quality) роботи ІС [5].

Працездатність ІС – час простою;

$$A = \tau_0 / \tau_{\hat{a}},$$

де τ_0 – операційний час (operation time), а τ_e – загальний витрачений час (elapsed time).

Продуктивність, як відношення

$$P = (x_i \tau_i) / \tau_e,$$

де x_i – кількість елементарних запитів, а τ_i – ідеальний часовий цикл, що розуміється як максимальна швидкість обробки стандартного i-*го* тестового запиту в даній ІС.

Очевидно, що продуктивність P не може перевищувати 100 %. Іноді "ідеальний цикл" з аналогічними виробничими системами називають "заводською характеристикою" NPCT (Name Plate Cycle Time).

Якість ЗІ, як узагальнена оцінка затримок в обслуговуванні даної ІС

$$Q = x_i / R,$$

де R – апостеріорне число відповідей, оцінюваних як релевантні (експертна оцінка).

Загальний вигляд оцінки ефективності ІС за методом *OEE* можливо представити як

$$OEE = \frac{\tau_0 \tau_i x_i^2}{\tau_e^2 R} \qquad (1)$$

Очевидно, що для оцінки ефективності згідно з (1) потрібна система постійних вимірювань основних параметрів.

Численні статистичні дані різних компаній показують, що значення *OEE* звичайно не перевищує 65,5%, працездатності – 86,0 %, продуктивності – 79,0 %, а якості – 96,5 %. У світі прийнятною оцінкою ефективності ІС за методом *OEE* вважається: 60% для ІС загального призначення та 85 % для спеціальних ІС.

Не дивлячись на постійне зростання продуктивності чипів й побудованих на їх основі ПТЗ, за оцінкою ефективності ІС облік тільки швидкодії ПТЗ вже не може задовольнити ні особу, що приймає рішення (ОПР), ні аналітиків спеціалізованих інформаційно-аналітичних систем (ІАС).

Візьмемо до уваги підхід АНБ США, яке, маючи найбільш високопродуктивні у світі ПТС, використовує в своїх ІС не більш 15% інформації, одержаної із всіх перехоплених повідомлень, оскільки ефективність ІС залежить не тільки від швидкодії системи, а й здатності та вміння аналітиків швидко оцінити важливість одержаної в процесі перехвату інформацію.

Слід також враховувати й особливості використаних в мережевих IP форматів (HTML XML), оскільки слова в назві сторінок, заголовках й тегах мають різні вагові коефіцієнти значущості, які, також як й слова "обрамлення", можуть уточнюватися в процесі пошуку.

Очевидно, що подібні спрощені методи оцінки ефективності ІС виправдовують себе при використанні щодо простих баз даних або інформаційних ресурсів. В процесі збільшення ступеня інформаційного поліморфізму та мультимедійності, подібні методики вже можуть використовуватися тільки для найгрубіших оцінок. При створенні сховищ складно-структурованої інформації, організованої на основі семантичних мереж, особливу роль починають виконувати внутрішні інформаційні зв'язки між вузлами цих мереж.

Оцінка ефективності ІЗ ІБ на підприємстві з погляду релевантності, що зберігається з використаної в ІС інформації, може бути формально описана як "задача про суміш" лінійного програмування, інформаційний вміст якої в системі визначається таким чином.

Одержавши задачу T, що розуміється в аспекті інформаційного пошуку як множина запитів $\{q_j\}$ до $ІЗ$ ІБ $j \in \{1,2,.....,n\}$ – клас запиту, аналітик формує та планує проведення цих запитів (запросний пул), беручи до уваги, що кожний запланований запит $j-го$ класу повинен мати пошукову затримку, яка не перевищує τ_j.

Для кожного класу запитів аналітик визначає релевантність r_j, виходячи з набору ключових слів, заданих наочною та проблемною областями задачі T, причому сумарна пошукова затримка не повинна перевищувати $T_{\max}$.

У цих термінах і визначеннях задача оптимізації ефективності ІЗ полягає в оптимізації кількості x_j запитів $\{q_j\}$-го класу, так, щоб сумарна релевантність була максимальною до обмеження на сумарний час всіх затримок

$$\max \sum_j r_j x_j,\ j \in \{1,2,.....,n\} \qquad (2)$$

$$\sum_j \tau_j x_j \le T_{\max},\ j \in \{1,2,.....,n\} \qquad (3)$$

$x_j \ge 0$, x_j – ціле число

Приведена нами вище формалізація (2 – 3) у вигляді "задачі про суміш" ставила у відповідність класам запитів апріорну узагальнену релевантність r_j та пошукову затримку τ_j, не деталізуючи структуру самих запитів, що може дати в результаті корисні, але достатньо узагальнені оцінки

В зв'язку з цим пропонується уточнена математична модель, в якій структура запиту враховує пов'язані з ним пошукові затримки ІС ІБ на підприємстві.

Для цього введемо наступні позначення:

$q_j = \{d_{ij},....,d_{sj}.....,d_{pj}\}$ – структура j-го класу запитів, як кортежу затримок d_i i–го типу;

a_{ij} – кількість затримок i-го типу в запиті j - го класу;

b_i – обмеження знизу на кількість затримок i-го типу в задачі T;

τ_j – значення затримки запиту j-го класу (експертна оцінка, виміри, тести);

t_j – фіксована затримка ПТЗ виконання запиту j-го класу;

x_j – кількість запитів j-го класу в задачі T.

Задача оптимізації полягає в мінімізації часу рішення задачі з урахуванням рівня релевантності, встановленого при рішенні задачі 4.9 – 4.10, а саме:

$$\min \sum_j \tau_j(x_j), \quad j \in \{1,2,.....,n\} \qquad (4)$$

$$\sum_j a_{ij} x_j \geq b_i, \quad i \in \{1,2,.....,m\}, \quad x_j \geq 0 \qquad (5)$$

де

$\tau_i(x_j) =$ (6)

При введенні верхньої межі $x_j \leq k_j$, $j \in \{1,2.....,n\}$ задача приймає вигляд:

$$\min \sum_j (\tau_j x_j + t_j y_j), \; j \in \{1,2.....,n\}.$$

$$y = \begin{cases} 0 & \text{при} \quad 0 \leq x_j \leq k_j y_j \\ 1 & \text{в протилежному випадку} \end{cases} \qquad (7)$$

Приведена вище формалізація (4.9 – 4.11) у вигляді "задачі про суміш" ставила у відповідність класам запитів апріорну релевантність, проте, як вже наголошувалося, отримання її чисельного значення вкрай утруднене складністю вимірів та відсутністю експертних оцінок.

Висновок

Тому для оцінки ефективності ІЗ ІБ на підприємстві необхідно варіювати значеннями різних параметрів інших пошукових затримок з метою оптимізації критерію ефективності, що враховує взаємовиключні вимоги максимізації або мінімізації.

Список літератури

1. Мала гірнича енциклопедія. В 3-х т. / За ред. В. С. Білецького. – Донецьк: «Донбас», 2004.

2. Советский энциклопедический словарь / Гл. ред. А.М. Прохоров. – 4-е изд. – М.: Сов.энциклопедия, 1989.– 1632 с.

3. Хорошко В. А. Модель системы защиты информации / В.А. Хорошко // Захист інформації, №1, 1999. – С.5 – 11.

4. Сяо Д. Защита ЕВМ / Д. Сяо : пер. с англ. Д. Керр, В. Медник. – М.: Мир, 1982. – 297 с.

5. Рабунец П. Общая эффективность оборудования / П. Рабунец. – М.: ИКСИ, 2007. – 120 с.

6. Петренко С.А. Защита корпоративных сетей Internet / Intranet от несанкционированного доступа / Петренко С.А. // Read.me, № 3, 2001. – С. 34–37

7. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.

8. Петренко С.А. Технология распределенных межсетевых экранов: Эффективная защита корпоративных серверов от несанкционированного доступа / Петренко С.А. // Read.me, № 10, 2000. – С. 14 – 17.

9. Петренко С.А. Реорганизация корпоративных сетей безопасности / С.А. Петренко // Конфидент, № 1, 2002. – С. 30 – 36.

10. Зегжда Д.П. Основы безопасности информационных систем / Д.П.Зегжда, А.М.Ивашко. – М.: Горячая линия – Телеком, 2000. – 452 с.

Рецензент: Дудикевич В.Б.
Надійшла