УДК 681.3

О.П. Дóренський[1], С.Б. Воропай[2]

[1]*Кіровоградський національний технічний університет, Кіровоград*
[2]*Департамент ФРБО Міністерства внутрішніх справ України, Київ*

ДО ПИТАННЯ ВИЗНАЧЕННЯ ЧАСТКОВИХ ПОКАЗНИКІВ МАТРИЦІ ОЦІНОК ТА КОЕФІЦІЄНТІВ ВІДНОСНОЇ ВАЖЛИВОСТІ ВИМОГ ДО ПАРАМЕТРІВ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

Розглядаються питання дослідження та оптимізації моделі системи комплексного оцінювання показника якості системи забезпечення безпеки інформації на основі матриці оцінок. Запропоновано, використовуючи метод визначення коефіцієнтів відносної важливості вимог та часткових показників оцінки безпеки інформації, усунути виявлені недоліки системи, що, як показали емпіричні досліди практичної реалізації моделі, дає можливість значно зменшити похибку результуючої комплексної оцінки показника якості системи забезпечення безпеки інформації.

система забезпечення безпеки інформації, безпека інформації інформаційної системи, комплексна оцінка рівня безпеки інформації

Вступ

Існуючі методики та моделі систем визначення рівня безпеки інформації інформаційної системи (ІС), яка забезпечується функціонування системи забезпечення безпеки інформації (СЗБІ), не дають точної об'єктивної (дискретної) її оцінки [1]. Тобто результуюча величина оцінки має похибку, яка не є сталою та залежить від ряду факторів. Це пов'язано з реалізацією алгоритмів оцінювання показника якості СЗБІ на основі суб'єктивної експертної інформації, яка в більшості випадків є інтуїтивною й залежною від рівня кваліфікації експерта. Саме тому отримана комплексна оцінка рівня безпеки інформації ІС може не відповідати дійсному стану речей. Це може призвести до прийняття невірних проектних рішень під час побудови або під час оцінювання вже існуючої СЗБІ з метою оновлення її функціональних блоків. Результатом цього може бути зниження стійкості СЗБІ до загроз та, відповідно, незадовільний рівень безпеки інформації ІС [1, 2].

Постановка проблеми. Однією з основних задач під час оцінювання критерія якості СЗБІ є експертна оцінка його часткових показників та визначення рівня важливості вимог до параметрів СЗБІ [3]. Досить проблематичним є також представлення якісної величини показника у кількісному виді: деякі показники є занадто об'ємними для їх оцінки експертом, що є причиною похибок у визначенні їх величини. Тому постає задача, яка потребує розв'язку: розробка більш досконалого та ефективнішого за існуючі методи отримання часткових показників якості та коефіцієнтів відносної важливості вимог до параметрів СЗБІ.

Аналіз літератури. У роботі [2] запропоновано методику визначення показника якості СЗБІ на основі матриці оцінок, елементами якої є часткові показники. Запропоновано метод визначення його кількісної характеристики та методи визначення коефіцієнтів важливості вимог до параметрів СЗБІ [5], які через ряд їх недоліків дають відповідні вихідні величини з досить високою ймовірністю похибки [6].

Формулювання цілей. Метою проведення досліджень є розв'язок задачі оптимізації існуючих моделей комплексної оцінки якості СЗБІ на основі матриці оцінок, що дасть можливість отримати більш досконалу модель одержання оцінки безпеки інформації ІС.

Основна частина

Якість СЗБІ визначається ступенем виконання вимог, які висуваються до СЗБІ. У основу оцінки якості СЗБІ пропонується покласти вихідні дані, представлені у вигляді матриці оцінок (знань), вхідні дані якої встановлюються експертом та за даними якої створюється потік даних для їх подальшої обробки відповідними методами (системою).

В дослідженні [2] запропоновано формувати матрицю оцінок на основі лінгвістичних (інтермальних) оцінок окремих елементів. Оскільки часткові показники мають якісний характер і не мають точного кількісного вимірювання, запропоновано їх оцінювати за принципом термометра (рис. 1). Будова матриці оцінок [2] , яка складається з K елементів, полягає в логічному об'єднанні показників блоків "Основи", "Напрями", "Етапи". У загальному випадку кількість елементів матриці $K = O_i \cdot H_j \cdot M_k$, де O_i – показники блоку "Основи", H_j – "Напрями", M_k – "Етапи" ($K = 140$). Блок показників O_i дозволяє виділити наступну групу часткових показників: нормативно-правова та наукова база; структура та задачі органів; організаційні заходи й методи (політика безпеки); програмно-технічні способи та засоби. Блок H_j: захист об'єктів корпоративних систем; захист проце-

сів, процедур та програм обробки інформації; захист каналів зв'язку; пригнічення електромагнітних випромінювань; керування системою захисту. Блок M_k: визначення інформації, яка підлягає захисту; виявлення повної множини потенційно можливих загроз та каналів витоку інформації; оцінка ризиків інформації; визначення вимог до системи захисту; вибір засобів захисту; впровадження та організація використання обраних заходів, способів та засобів захисту; здійснення контроля цілісності [2].

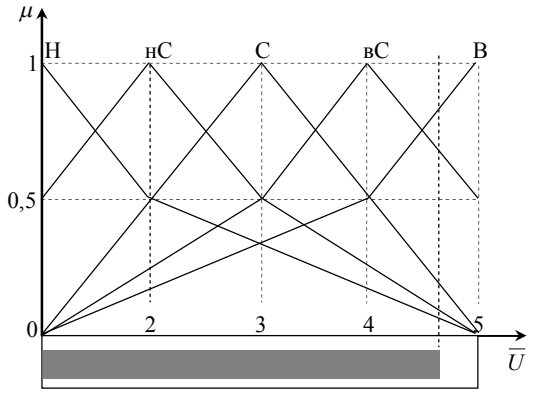

Рис. 1. Оцінювання часткових показників за принципом термометра

Тоді показник якості СЗБІ Q має вигляд

$$Q = \sum_{k=1}^{n}\sum_{j=1}^{l}\sum_{i=1}^{r} z_{kji} \Big/ (n \cdot l \cdot r), \qquad (1)$$

де $z_{kji} = \begin{cases} 1, & \text{при } q_{kij} > q_{kij}^{T}, \\ 0 & \text{при } q_{kij} < q_{kij}^{T}. \end{cases}$, q_{kij} та q_{kij}^{T} – дійсне та дане значення часткових показників відповідно, n – кількість рядків, l – кількість підстовпців [2], r – кількість стовпців матриці оцінок.

Для матриці оцінок часткових показників [2] $n = 5$, $l = 4$, $r = 5$.

Виходячи з (1), оцінка якості СЗБІ має вигляд

$$Q = \sum_{i=1}^{m} \omega_i q_i , \qquad (2)$$

де ω_i – ваговий коефіцієнт i -го показника, при чому $\sum_{i=1}^{m} \omega_i = 1$, $\omega_i > 0$, $i = \overline{1,m}$ [3].

Проте велика кількість елементів матриці оцінок (m) може призвести до втрати об'єктивності визначення вагових коефіцієнтів. Тому пропонується задавати вагові коефіцієнти стовпців, рядків та підрядків матриці оцінок

$$Q = \sum_{k=1}^{n} \omega_k \sum_{j=1}^{l} \omega_j \sum_{i=1}^{r} \omega_i q_{kji} , \qquad (3)$$

де $\sum_{k=1}^{n} \omega_k = 1$, $\sum_{j=1}^{l} \omega_j = 1$, $\sum_{i=1}^{r} \omega_i = 1$.

Ступінь виконання кожної вимоги визначається як виконана ($X_j = 1$) або не виконана вимога ($X_j = 0$, $j = 1,m$). Якщо важливість вимоги не враховується, якість СЗБІ оцінюють співвідношенням

$$W = \sum_{j=1}^{m} X_j \Big/ m , \qquad (4)$$

при $0 \le W \le 1$.

Якщо ж ступінь виконання вимоги оцінюють з урахуванням важливості вимоги, то показник W оцінюється співвідношенням

$$W = \sum_{j=1}^{m} a_j x_j , \qquad (5)$$

де $0 \le a_j \le 1$; $\sum_{j=1}^{m} a_j = 1$.

В [2] також досліджено оцінювання ступеня виконання вимог за бальною шкалою. Застосувавши найпоширенішу п'ятибальну шкалу $B_j = 5$ – відмінно, $B_j = 4$ – добре, $B_j = 3$ – задовільно, $B_j = 2$ – незадовільно, $B_j = 1$ – повністю незадовільно, якість СЗБІ визначається середнім балом

$$\overline{B} = \sum_{j=1}^{m} b_j \Big/ m , \qquad (6)$$

при $1 \le \overline{B} \le 5$, $1 \le \overline{B} \le 5 j = \overline{1,m}$.

За умови додаткового визначення важливості кожної вимоги якість СЗБІ визначається виразом

$$\overline{B} = \sum_{j=1}^{m} a_j b_j , \qquad (7)$$

при $0 \le a \le 1$, $\sum_{j=1}^{m} a_j = 1$.

Таким чином, оцінювання якості СЗБІ пропонується виконувати згідно формул (6) та (7)

$$\overline{B} = \sum_{j=1}^{m} q_j \Big/ m , \qquad (8)$$

а з урахування коефіцієнта важливості вимоги до параметра СЗБІ

$$\overline{B} = \sum_{j=1}^{m} a_j q_j . \qquad (9)$$

Дослідження та детальний аналіз методики оцінювання показника якості СЗБІ [2] дало можливість виявити наступні недоліки: обраний принцип встановлення величини часткових показників – термометра – не дає можливості об'єктивно оцінити рівень показника, оскільки під час оцінювання одного й того ж показника декількома експертами величини даного показника можуть бути різними, т.я. кожен експерт має різну інтуїтивно сформовану оцінку якості даного показника; величини показника

важливості вимоги та заданий рівень визначається загальною суб'єктивною оцінкою експерта і може не відповідати дійсності, що є загрозою неточної комплексної оцінки якості СЗБІ в цілому [6].

Для визначення величини коефіцієнта відносної важливості вимог до параметрів СЗБІ ω_j застосовується метод визначення коефіцієнта відносної важливості вимоги до параметрів СЗІ [5]. Але він є досить трудоємним з точки зору практичного використання експертом під час оцінювання рівня безпеки ІС. Тому запропонуємо визначати ω за допомогою ваги класа загрози, якій протидіє заданий параметр СЗБІ [1]. Тобто, її значення визначимо зі співвідношення

$$\omega_j = \begin{cases} 0.11, & \text{при } i = 1; \\ 0.11, & \text{при } i = 2; \\ 0.13, & \text{при } i = 3; \\ 0.65, & \text{при } i = 4; \end{cases}$$

де i – клас загрози (I-IV), на протидію якої направлений параметр СЗБІ [1].

У дослідженні [4] запропоновано задачу визначення коефіцієнта відносної важливості вимоги до параметра СЗБІ ω_j можна вирішити за допомогою ймовірнісного підхода, тобто

$$\omega_j = \sum_{i=1}^{4} P_{i\ загр} \cdot \sum_{j=1}^{4} \sum_{k=1}^{m} p_{jk},$$

де $P_{i\ загр}$ – ймовірність появи загрози i-того класу, p_{jk} – ймовірність успішної протидії k-й загрозі i-того класу.

Але визначення коефіцієнтів відносної важливості вимоги до параметрів СЗБІ методом [4], як і методом [2], є досить трудоємним і обтяжливим у практичному застосуванні та реалізації. Тому пропонується для визначення ω_j використовувати метод [1].

Таким чином, експерт має можливість досить просто, зручно та точно визначити коефіцієнт важливості вимоги до параметра, який він оцінює. Зокрема, даний метод значно ефективніший для програмної реалізації та зручного подання даної інформації експерту.

Дійсно, оцінювання часткових показників елементів матриці оцінок за принципом термометра дає можливість використовувати показник оцінки СЗБІ як адитивний показник, який для кількісної оцінки якості системи дозволяє визначити кількість виконаних часткових показників. В [2] даний показник представлено у вигляді суми вагових нормованих часткових показників (2). Але альтернативним та більш раціональним розв'язком даної задачі та усунення відповідного недоліка буде використання підтаблиці оцінок заданого критерія.

Тобто, задача загального оцінювання часткового показника розбивається експертом на підзадачі у необхідній кількості для легкого та максимально точного оцінювання кожної з них. Відповідно середній бал (оцінка) всіх підзадач виражатиме кількісний рівень часткового показника, який оцінюється

$$q_j = \sum_{i=1}^{n} p_i \Big/ \tau, \qquad (10)$$

де p_i – рівень виконання характеристики (підзадачі), n – кількість характеристик часткового показника.

Таким чином, декомпозиція задачі оцінювання часткового показника q_j на підзадачі (характеристики) p_i забезпечує точне визначення його рівня, оскільки оцінювання кожної характеристики поодинці дає її об'єктивну оцінку, а не приблизно-інтуїтивну. Якщо дана характеристика після проведення її декомпозиції все-одно занадто об'ємна для проведення її оцінювання, пропонується здійснити другий рівень її розбиття на підзадачі. Крім того, використання запропонованого методу дасть можливість уникати помилок експерта, а за умови невідповідності рівня безпеки системи заданому – аналізувати невраховані або неправильно оцінені показники.

Ще однією перевагою декомпозиції q_j на p_i є можливість виявлення "слабких" місць СЗБІ: якщо $p_i = 0$, а ω_j має досить високий рівень, це свідчить про нагальну необхідність забезпечення даної характеристики. А метод [2] такої можливості не дає, в результаті чого важливі характеристики системи ЗБІ можуть бути не реалізовані, в результаті чого СЗБІ матиме вразливі місця, виявлення зловмисником (зловмисниками) яких дасть можливість унеможливити виконання функцій СЗБІ та призвести, відповідно, до небезпеки інформації ІС [1, 5, 6].

Практична програмна реалізація запропонованих методів за допомогою динамічного списку з відповідними частковими показниками (характеристиками) відповідного елемента матриці оцінок експертної системи комплексного оцінювання системи захисту інформації [5]. Результати експериментального випробування оптимізованої системи оцінки рівня безпеки інформації ІС навчально-методичного відділу КірЮІ Харківського національного університету внутрішніх справ (м. Кіровоград) показали значно меншу похибку отриманої оцінки якості СЗБІ, здійсненої за експертними даними п'яти експериментів (рис. 2).

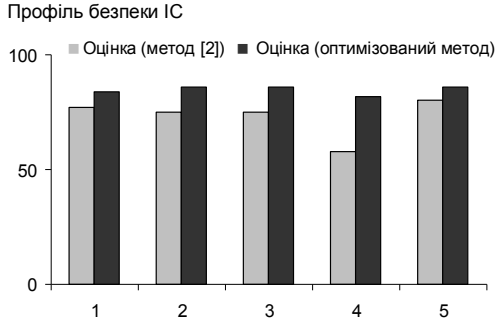

Рис. 2. Рівень досягнутої безпеки ІС [6] на основі різної експертної інформації

Точність заданих показників системи [2] сягала 73,0%, оптимізованої – 84,8, при цьому відхилення від середнього значення становить 6,0% та 1,44% відповідно [6]. Таким чином, застосування оптимізованої методики на 11,8% підвищує ефективність системи оцінювання якості СЗБІ. Про це свідчить одержаний графік результатів роботи дослідного зразка системи (рис. 3): результуюча лінія 2 вказує на значно вищу точність результатів оптимізованої системи [6].

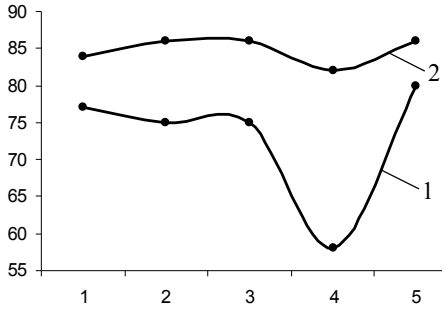

Рис. 3. Графік оцінок ІС системи [5] (1) та оптимізованої системи (2)

Це дає підстави стверджувати про значно вищу ефективність запропонованих методів визначення коефіцієнта відносної важливості вимог до параметрів СЗБІ й оцінювання часткового показника оцінки безпеки інформації та, відповідно, розв'язок поставленої задачі.

Висновки

За результатами дослідження можна зробити наступні висновки:

1) у роботі досліджено та проведено детальний аналіз методики визначення комплексного показника якості функціонування СЗБІ [2];

2) за результатами досліджень запропоновано оптимізацію методів оцінювання показника якості СЗБІ, зокрема визначення кількісної величини часткового показника якості параметра СЗБІ;

3) запропоновано більш ефективний метод визначення коефіцієнтів відносної важливості вимог до параметрів СЗБІ;

4) наведено одержані результати проведеного експериментального дослідження впроваджених у систему оцінювання якості СЗБІ запропонованих методів, які показали на 4,2% зменшення середнього відхилення оцінки та на 11,8% вищу ефективність оптимізованої системи комплексного оцінювання якості СЗБІ, що й доводить практичну цінність застосування запропонованих методів.

Список літератури

1. Дóренський О.П. Дослідження потенційних загроз безпеці інформації інформаційної системи та аналіз їх класифікаційного поділу. // Зб. наукових праць Кіровоградського національного технічного університету. – Кіровоград: КНТУ, 2007. – Вип. 18. – С. 150-157.

2. Домарєв В.В. Оцінка застосування засобів технічного захисту інформації в інформаційних системах // Захист інформації. – 2004. –Вип. 22. – С. 8-13.

3. Гудкін Л.С. Оптимизация радиоэлектронных устройств по совокупности показателей качества. – М.: Радио, 1975. – 367 с.

4. Дóренський О.П. Метод визначення коефіцієнтів відносної важливості вимог до параметрів системи забезпечення безпеки інформації // Захист інформації. – К.: ДУІКТ, 2007. – С. 34-41.

5. Домарев В.В. Безопасность информационных технологий. Системный подход. – К.: ООО "Тид "ДС", 2004. – 992 с.

6. Волошанюк В.Г., Дóренський О.П. Про результати оптимізації системи оцінювання якості системи забезпечення безпеки інформації. // Зб. тез доповідей ІІІ Міжвузівського науково-практичного семінару "Комбінаторні конфігурації та їх застосування". – Кіровоград: ДЛАУ, 17-18 квітня 2007 р. – С. 16-18.

Надійшла до редколегії 3.08.2007

Рецензент: д-р фіз.-мат. наук, проф. Ю.І. Волков, Кіровоградський національний технічний університет, Кіровоград.