

ББК γ 973.2-021.2+ γ 811-021.2+ γ 973.2-018.4

УДК 681.3:004

М.М. Браїловський, В.О. Хорошко, О.В. Хорошко

ОПТИМІЗАЦІЯ ВИБОРУ ПАРАМЕТРІВ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Розглянуто критерій вибору показників якості параметрів складної системи. Запропонований критерій дозволяє робити оцінку систем в діапазоні можливих відхилень приватних критеріїв і завдяки цьому додатково враховувати ступінь погіршення одних параметрів за рахунок поліпшення інших.

Створення систем захисту інформації (СЗІ) і оцінки якості їхньої працездатності передбачає вирішення широкого кола різнопланових задач. Оцінку якості вибору їхніх параметрів слід здійснювати на базі критерію, який дозволяв би оцінювати застосування однієї і тієї ж системи в різних умовах використання або різних систем при вирішенні однопланових задач.

Метою даної роботи і є вибір такого критерію. Прагнення поліпшити в процесі проектування системи захисту інформації СЗІ один з показників якості її функціонування призводить до неминучої зміни одного або декількох показників. Тому і не вдається строго обґрунтувати вигляд результуючої цільової функції (визначити узагальнений показник якості) об'єктивним шляхом. В таких випадках однією з можливостей є застосування лінійного критерію [1].

Припустимо, що якість функціонування СЗІ описується сукупністю приватних критеріїв, які необхідно мінімізувати $\vec{K} = \langle K_1, K_2, \dots, K_m \rangle$. Знайдемо відносні відхилення приватних критеріїв від екстремальних (мінімального і максимального) значень:

$$K_{\max}^i = \frac{K_i(CZI) - K_i^{\min}(CZI)}{K_i^{\max}(CZI)}, \quad i = \overline{1, m}. \quad (1)$$

Тоді вибрана СЗІ буде залишатися оптимальною за сукупністю приватних критеріїв, якщо вони характеризуються сукупністю відносних відхилень, які мають найменші значення. Позначивши оптимальний варіант системи захисту інформації як C_0 , запишемо в формалізованому вигляді цю задачу таким чином:

$$\begin{aligned} K_{\max}^i(C_0) &< K_{\max}^i(C); \\ C, C_0 &\in C_{\text{СД}}, \end{aligned} \quad (2)$$

де $K_{\max}^i = \max \{ K_i^i \}; i = \overline{1, m}$ – найбільше з відносних відхилень, які розраховують по формулі (1); $C_{\text{СД}}$ – безліч СЗІ (строго допустимих), сукупності умов, що задовольняють застосування системи і обмеження на структуру і значення основних параметрів.

До умов застосування СЗІ відносяться, наприклад, діапазон робочих температур, глибина захисту і т. ін.

Запропонований критерій відрізняється від наведених в роботах [1] і [2] тим, що дозволяє робити оцінку СЗІ в діапазоні можливих відхилень приватних критеріїв і завдяки цьому додатково враховує ступінь погіршення одних параметрів СЗІ за рахунок поліпшення

інших. Однак при використанні критерію $K_i^{\min} \ll K_i^{\max}$ перевага може бути віддана такій СЗІ з пари існуючих, яка при незначному кращому (меншому) значенні одного показника якості володіє значно гіршими іншими показниками у порівнянні з відповідними показниками якості іншої СЗІ. В цьому випадку критерій, що розглядається, має той же недолік, що і критерії, наведені в роботах [1] і [2]. Враховуючи це, модифікований мінімаксний критерій доцільно використати при виборі оптимального варіанта із сукупності СЗІ однакового технологічного виконання.

Мінімаксний критерій (2) можна навести також у вигляді:

$$K_p = f_p(K_1, \dots, K_i, \dots, K_m) = \min; \quad (3)$$

$$C \in C_{\text{сд}},$$

$$\text{де } f_p(K_1, \dots, K_i, \dots, K_m) = \max \frac{K_i - K_1^{\min}}{K_1^{\max}}, \dots, \frac{K_i - K_i^{\min}}{K_i^{\max}}, \dots, \frac{K_m - K_m^{\min}}{K_m^{\max}}. \quad (4)$$

Система захисту інформації C_0 , що визначається розв'язанням задачі (3), (4) і буде оптимальною. З формули (3) слідує, що мінімаксний критерій можна вважати різновидом критерію, оснований на мінімізації результуючої цільової функції, вигляд якої відповідає виразу (4).

Із залежностей (3) і (4) бачимо, що мінімаксний критерій забезпечує найкраще (найменше) значення із сукупності найгірших (найбільших) нормованих показників якості. Тому всі приватні показники якості СЗІ слід привести до стаціонарного вигляду. Показник якості K_i буде вважатися стандартним, якщо він задовольняє умову $K_i \geq 0$, де $i = \overline{1, m}$, і, чим менше значення K_i , тим краще вибраний варіант СЗІ. Якщо деякий показник якості K_i^* не є стандартним, то його завжди можна привести до вигляду K_i . Наприклад, якщо невід'ємний показник якості може змінюватися в межах $K_{i\min}^* \leq K_i^* \leq K_{i\max}^*$ і, чим більше значення K_i^* , тим краще СЗІ, то як еквівалентний йому стандартний показник якості слід вибрати значення $K_i = K_{i\max}^* - K_i^*$ або (за умови $K_{i\max} \rightarrow \infty$) $K_i = \frac{1}{K_i^*}$.

Отже, K_i^* є стандартним показником якості, який дає можливість здійснювати порівняння СЗІ у різних умовах експлуатації або порівнювати різні системи, які працюють на одному об'єкті, між собою.

Припустимо, що СЗІ (типорозмір) параметричного ряду характеризується вектором розмірністю m :

$$\vec{K}_j = \langle K_{j1}, \dots, K_{ji}, \dots, K_{jm} \rangle; j = \overline{1, n},$$

де j – порядковий номер типорозміру; K_{ji} – приватний критерій якості j -го типорозміру, приведений до стандартного вигляду.

При цьому потреби в кожному типорозмірі параметричного ряду задаються однією з координат вектора \vec{K}_j з урахуванням меж K_j^{\min} і K_j^{\max} можливих значень критеріїв, де K_j^{\min} – найменше, а K_j^{\max} – найбільше значення i -ї координати вектора за всіма значеннями

j^i . Типорозміри вхідного змінного ряду упорядковані за найбільш значущим приватним критерієм, якому відповідає порядковий номер координати $i = 1$. Таким чином, можна записати:

$$K_{11}^{\max} \geq K_{21} \geq K_{j1} \geq K_{(n-1)1} \geq K_{n1}^{\max}; j = \overline{1, n}.$$

Будемо також вважати заданим набір опорних векторів $K_r^o (r = \overline{1, R})$, кожний з яких характеризує якість СЗІ, виконаної в рамках однієї схемотехнічної реалізації. Основні параметри цих СЗІ можуть бути оцінені за результатами аналізу моделей і тенденцій розвитку систем заборони і повинні на час реалізації вимог параметричного ряду відповідати досягнутому рівню розвитку. Тоді шляхом відповідності опорного і вхідного набору векторів за координатами, які відповідають значущому критерію якості СЗІ, інтервал $[K_{11}^{\max}, K_{n1}^{\min}]$ можна розбити на дрібніші інтервали $[K_{11}^{\max}, K_{11}^0], [K_{11}^0, K_{21}^0], \dots, [K_{(R-1)1}^0, K_{R1}^0]$, де $K_{R1}^0 \leq K_{n1}^{\min}$.

Таким чином, можливе повне перекриття інтервалу $[K_{11}^{\max}, K_{n1}^{\min}]$ і задоволення всіх вимог до системи.

Системи захисту інформації з опорними критеріями якості утворюють опорний параметричний ряд, який в загальному випадку не є оптимальним. Це пов'язано з тим, що один або декілька параметрів системи можуть перевищувати необхідні значення. В той же час для забезпечення високого технічного рівня розробок необхідно створити СЗІ, параметри яких відповідали б максимально досягнутому розвитку техніки. Компромісне рішення при цьому дозволяє оптимізувати параметричний ряд на основі мінімаксного критерію. Для інтервалу $(K_{(r-1)1}^0, K_{r1}^0)$, де $r = \overline{1, R}$ вирішуємо S_{\max} задачі математичного програмування:

$$\min_{K_j \in \Omega_r^s} K^1(K_j) = \min_{K_j \in \Omega_r^s} \max \left(\frac{K_{ji} - K_i^{\max}}{K_i^{\max}} \right); i = \overline{1, m}, \quad (5)$$

де $K^1(K_j)$ – найбільше з відносних відношень приватних критеріїв, що є координатами вектора \vec{K}_j від екстремальних значень; Ω_r^s – множина векторів вхідного параметричного ряду, яка задовольняє умову $K_{ji}^s \geq K_{j1} \geq K_r^0$. Тут K_{j1}^s – найбільш значущий приватний критерій оптимальної (в смислі мінімаксного критерію) СЗІ.

Механізм утворення множин Ω_r^s можна представити таким чином. Спочатку розв'язують вираз (5) на інтервалі $(K_{(r-1)1}^0, K_{21}^0]$. В результаті рішення визначається перша мінімаксна система і найбільш значущий критерій, який має значення $K_{j1}^1 (S=1)$. Ця СЗІ (з ряду розглянутих) характеризується мінімаксним відносним відхиленням і відносно сукупності приватних критеріїв. Однак жорсткі обмеження, які накладаються на найбільш значущий параметр СЗІ, в загальному випадку не дозволяють розглядати його як єдиний типорозмір, що задовольняє всі вхідні вимоги. Тому задачу розв'язують повторно на інтервалі $(K_{(r-1)1}^0, K_{r1}^0]$ і визначають другу СЗІ, найбільш значущий критерій якої має

значення $K_{r1}^2 (S = 2)$. Процес розв'язання виразу (5) триває до тих пір, доки опорний типорозмір не виявиться серед мінімаксних СЗІ або не буде єдиним елементом множини Ω_r^* . Очевидно, що найбільшому значенню змінної S відповідає число типорозмірів, які утворюють на інтервалі $(K_{(r-1)1}^0, K_{r1}^0]$ оптимальний параметричний ряд СЗІ. Для формування ряду, що задовольнить весь діапазон вимог, вираз (5) розв'язують роздільно на кожному інтервалі $(K_{(r-1)1}^0, K_{r1}^0]$, де $r = \overline{1, R}$.

Особливістю оптимізації, що пропонується, є наявність змішаних обмежень на область застосування кожного типорозміру: жорсткі обмеження у вигляді нерівностей накладаються на найбільш значущий параметр СЗІ; на інші параметри накладаються жорсткі обмеження у вигляді відносних втрат, що в процесі оптимізації мінімізуються.

Список літератури

1. Мамиконов А.Г., Кульба В.В., Шилков А.Б. Достоверность, защита и резервирование информации в АСУ. – М.: Энергоатомиздат, 1986. – 386 с.
2. Сигорский В. П. Математичний апарат інженера. – К.: Техніка, 1975. – 768 с.

Стаття надійшла до редакції 10 вересня 1998 року.

Микола Миколайович Браїловський (1972) закінчив Українську державну академію зв'язку в 1994 році. Інженер кафедри "Автоматизація прийому та обробки інформації". Спеціалізується в галузі технічного захисту інформації.

Mykola M. Brailovskyi (b. 1972) graduated from Ukrainian State Communication Academy (1994). Engineer of Automatic Reception and Processing of Information Department. Specializes in technical protection of information.

Володимир Олексійович Хорошко (1945), закінчив радіотехнічний факультет Київського інституту інженерів цивільної авіації у 1968 році. Доктор технічних наук, професор кафедри "Автоматизація прийому та обробки інформації". Має понад 150 наукових праць. Галузь наукових досліджень – обчислювальні комплекси, системи та мережі; захист інформації.

Volodymir O. Khoroshko (b. 1945) graduated from Kyiv Institute of Civil Aviation Engineers (1968). DSc (Eng), professor of Automatic Reception and Processing of Information Department. Author of more than 150 publications. Specializes in the fields of calculation complexes, systems and networks, protection of information.

Олексій Володимирович Хорошко (1973) закінчив радіотехнічний факультет Київського міжнародного університету цивільної авіації у 1996 році. Аспірант кафедри "Технічна електродинаміка". Спеціалізується у галузі технічного захисту інформації.

Olexyi V. Khoroshko (b. 1973) graduated from Kyiv International University of Civil Aviation (1996). Aspirant of Technical electrodynamics Department. Specializes in technical protection of information