

УДК 004.056.53

БАГАТОКРИТЕРІЙНИЙ СИНТЕЗ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Р. В. Грищук

Кандидат технічних наук, старший науковий співробітник
Науковий центр
Житомирський військовий інститут ім. С.П. Корольова
Національного авіаційного університету
пр. Миру, 23, м. Житомир, Україна, 10004
Контактний тел.: 093-575-34-96
E-mail: RuslanGRV@rambler.ru

І. А. Пількевич

Доктор технічних наук, професор, завідувач кафедри*
Контактний тел. (0412)-415-686, 067-39-787-39
E-mail: igor.pilkevich@mail.ru

В. О. Хорошко

Доктор технічних наук, професор
Кафедра безпеки інформаційних технологій
Інститут інформаційно-діагностичних систем
Національний авіаційний університет
пр. Космонавта Комарова, 1, м. Київ, Україна, 03058

В. І. Котков

Кандидат технічних наук, доцент*
Контактний тел. (0412)-22-94-08
E-mail: eko_univer@i.ua

*Кафедра моніторингу навколишнього природного середовища
Житомирський національний агроекологічний університет
бул. Старий, 7, м. Житомир, Україна, 10008

Розроблено сучасну технологію багатокритерійного синтезу систем інформаційної безпеки, що ґрунтується на застосуванні методу вкладних скалярних згорток, який адаптовано до вирішення відповідної проблеми. Застосування технології дозволяє враховувати не тільки усю множину вимог, що висувуються до системи інформаційної безпеки, але й одночасно дозволяє враховувати їх походження без обмеження на їх кількість

Ключові слова: система інформаційної безпеки, скалярна згортка, критерій оптимізації, багатокритерійний синтез, технологія

Предложена современная технология многокритериального синтеза систем информационной безопасности, которая основывается на применении метода вложенных скалярных сверток, адаптированного к решению соответствующей проблемы. Применение технологии позволяет не только учитывать все множество выдвигаемых требований к системе информационной безопасности, но и одновременно позволяет снять вопрос об учете их количества и природы происхождения

Ключевые слова: система информационной безопасности, скалярная свертка, критерий оптимизации, многокритериальный синтез, технология

Постановка проблеми

Створення прогресивних систем інформаційної безпеки (СІБ) невід'ємно пов'язано з вирішенням сукупності проблем, обумовлених багатокритерійним характером процесу забезпечення інформаційної безпеки [1–3]. При цьому багатокритерійність проявляється неповнотою й апріорною невизначеністю про склад та характер загроз безпеці інформації, потребою урахування значної кількості частинних критеріїв які, як правило, знаходяться в складних конфліктних взаємовідносинах і мають кількісне та якісне подання тощо [4]. Вказані особливості процесу забезпечення інформаційної безпеки значно обмежують можливості відомих методів оптимізації.

Аналіз останніх досліджень і публікацій

З аналізу фахової наукової літератури [1–9] та інших відкритих спеціалізованих джерел встановлено,

що проблемі синтезу СІБ приділяється значна увага провідних фахівців у галузі інформаційної безпеки. Але при цьому недоліком існуючої методології залишається високий ступінь суб'єктивізму одержуваних оцінок, який не в останню чергу обумовлений професійними якостями експерта з інформаційної безпеки – особи, що приймає управлінське рішення. Також удосконалення потребує технологія оптимального багатокритерійного синтезу параметрів СІБ за заданими властивостями.

Таким чином, у галузі інформаційної безпеки потреба у створенні нової, теоретично обґрунтованої та застосовуваної на практиці технології багатокритерійного синтезу СІБ є очевидною, а відповідна задача – актуальною та такою, що потребує свого розв'язання.

Основний зміст дослідження

Метою статті є розробка технології багатокритерійного синтезу систем інформаційної безпеки.

При класичній постановці багатокритерійної задачі оперують поняттям оптимізації векторного критерію. Як правило така оптимізація здійснюється за усією сукупністю формалізованих частинних критеріїв за відомими схемами. Наприклад за схемою згортки частинних критеріїв в один векторний критерій з подальшим пошуком оптимального – компромісного рішення тощо. Поряд з суттєвими перевагами такого підходу збільшення кількості частинних критеріїв та їх взаємообумовленість й конфліктна природа призводять до нечутливості відомих схем оптимізації до критеріїв з відносно малою питомою вагою. У результаті такі критерії фактично виключаються з процесу оптимізації та пошуку компромісного рішення. Такий підхід є неприпустимим при створенні сучасних СІБ, оскільки постійне підвищення вимог до системи обумовлює існування зліченної кількості ієрархічно впрограмованої множини частинних критеріїв.

Формалізація задачі. Нехай для створюваної СІБ усі властивості на $(j-1)$ -у рівні ієрархії задано $L^{(j-1)}$ -мірним вектором кількісних та якісних характеристик вигляду:

$$I^{(j-1)} = \{I_S^{(j-1)}\}_{S=1}^{L^{(j-1)}}, \quad j \in [2, m], \quad (1)$$

де $I^{(j-1)}$ – вектор частинних критеріїв на $(j-1)$ -у рівні ієрархії, який виступає компонентою, на основі якої оцінюється ефективність СІБ на j -у рівні;

j – рівень ієрархії частинних критеріїв;

$I_S^{(j-1)}$ – S -й частинний критерій $(j-1)$ -го рівня ієрархії, $S \in [1, L^{(j-1)}]$ ($L^{(j-1)}$ – кількість частинних критеріїв, за якими оцінюється ефективність СІБ на $(j-1)$ -у рівні ієрархії);

m – кількість рівнів ієрархії.

Компоненти векторного критерію $I^{(j-1)}$ (1) на $(j-1)$ -у рівні визначені в області

$$M^{(j-1)} = \left\{ I^{(j-1)} \left\{ 0 \leq I_S^{(j-1)} \leq I_{S \max}^{(j-1)}, S \in [1, L^{(j-1)}] \right\} \right\}, \quad (2)$$

де $I_{S \max}^{(j-1)}$ – обмеження, що задаються виходячи з фізичних міркувань.

Тоді багатокритерійна задача синтезу СІБ може бути формалізована у вигляді:

$$I^{(j)} \rightarrow \max. \quad (3)$$

Тобто, на j -му рівні ієрархії СІБ повинна забезпечувати максимальне наближення усієї ієрархічної системи критеріїв до свого екстремального – максимального значення.

В основу багатокритерійного синтезу СІБ покладено підхід [10], який вже знайшов своє місце при вирішенні широкого спектру задач захисту інформації у рамках вирішення проблеми інформаційної безпеки [11], що ніколи не робилося іншими авторами.

Метод розв'язання. На першому кроці, виходячи із заданої ієрархічної системи векторів (1), що визначає властивості СІБ, виділенню підлягають рівні ієрархії частинних критеріїв з подальшою побудовою їх структурної схеми та зазначенням взаємних зв'язків між ними.

На другому кроці здійснюється нормування частинних критеріїв. Для критеріїв заданих кількісно, наприклад $I_{01}^{(j-1)}, \dots, I_{0S}^{(j-1)}$, нормування здійснюється згідно з виразом:

$$I_{0S\theta}^{(j-1)} = \frac{I_{S\theta}^{(j-1)}}{I_{S\theta \max}^{(j-1)}}, \quad (4)$$

де $I_{S\theta \max}^{(j-1)}$ – максимальне значення $I_{S\theta}^{(j-1)}$ -го критерію при оцінюванні S -ї властивості $(j-1)$ -го рівня ієрархії для θ -ї властивості j -го рівня ієрархії та зведеними до одного принципу екстремізації – мінімуму. Тобто

$$I_S \rightarrow \min, \quad 0 \leq I_S \leq I_{S \max}, \quad I = \{I_{S \max}\}_{S=1}^L, \quad (5)$$

де I – вектор обмежень.

Для тих критеріїв, властивості яких задано якісно, кількісне значення нормованого частинного критерію $I_{0S\theta}^{(j-1)}$ (4) слід обирати з табл. 1.

Таблиця 1

Інтервальна обернена нормована фундаментальна шкала переходів

Ефективність СІБ (якісна оцінка)	Інтервал оберненої нормованої фундаментальної шкали оцінок $I_{0\theta}^{(j)}$ (кількісна оцінка)
абсолютно неефективна	1,0–0,7
недостатньо ефективна	0,7–0,5
ефективна	0,5–0,4
достатньо ефективна	0,4–0,2
абсолютно ефективна	0,2–0,0

Для практичних розрахунків кількісне значення нормованого частинного критерію $I_{0S\theta}^{(j-1)}$ (4) доцільно обирати, як середнє значення з визначеного інтервалу оберненої нормованої фундаментальної шкали переходів, що відповідає заданій якості (див. табл. 1).

На третьому, заключному кроці, оцінювання θ -ї властивості ефективності СІБ на j -у рівні ієрархії за заданими властивостями в цілому виражається задачею визначення скалярної згортки критеріїв на верхньому рівні ієрархії $I_0^{(j)}$ за нелінійною схемою компромісів [10], тобто

$$I_{0\theta}^{(j)} = 1 - L_{\theta}^{(j-1)} \left\{ \sum_{S=1}^{L^{(j-1)}} [1 - I_{0S\theta}^{(j-1)}]^{-1} \right\}^{-1}, \quad \theta \in [1, L^{(j)}], \quad j \in [2, m]. \quad (6)$$

де $I_{0\theta}^{(j)}$ – нормований частинний критерій при оцінюванні θ -ї властивості альтернативи на j -у рівні ієрархії, що мінімізується, $I_{0\theta}^{(j)} \in [0; 1]$;

$L_{\theta}^{(j-1)}$ – кількість альтернатив;

$I_{0S\theta}^{(j-1)}$ – компоненти нормованого вектора $I_0^{(j-1)}$, що застосовуються при оцінюванні θ -ї властивості альтернативи на j -у рівні ієрархії;

$L^{(j)}$ – кількість властивостей, що оцінюються на j -у рівні.

Ітераційна послідовність операцій зваженої скалярної згортки критеріїв кожного з рівнів ієрархії – від нижнього до верхнього на основі методу вкладних скалярних згорток [10] дозволяє здійснити синтез СІБ

за одержаною оцінкою ефективності системи за заданими властивостями в цілому, тобто

$$\{I_{05}^{(j-1)} \rightarrow I_0^{(j)}\}, j \in [2, m]. \tag{7}$$

Співставлення кількісної оцінки (7) з інтервальною оберненою нормованою фундаментальною шкалою (див. табл. 1) дозволяє одержувати якісну оцінку ефективності СІБ, що створюється за заданими властивостями за результатами багатокритерійного синтезу (3).

Демонстрація можливостей підходу. Нехай створювана СІБ описується вектором кількісних та якісних характеристик (табл. 2). Потрібно здійснити багатокритерійний синтез СІБ (3) та, виходячи з розрахованих показників за критерієм ефективності (7), обрати найкращий варіант побудови системи.

Таблиця 2

Профіль системи інформаційної безпеки

№ з/п	Критерії	Показники		
		СІБ-1	СІБ-2	СІБ-3
1.	Середня ймовірність перебування СІБ в захищеному стані під впливом методів захисту інформації	0,66	0,68	0,9
2.	Середня інтенсивність перевірок якості функціонування СІБ	0,5251	0,7325	0,2514
3.	Середня інтенсивність нападу (атак) на СІБ	0,9645	0,9	0,2514
4.	Середня інтенсивність відмов СІБ	0,0027	0,0027	0,0027
5.	Середня інтенсивність знаходження вразливостей СІБ	0,0328	0,328	0,028
6.	Середня інтенсивність усунення вразливостей СІБ	0,0328	0,328	0,0328
7.	Середня інтенсивність оновлення сигнатур вірусів в СІБ	1	1	1
8.	Рівень захищеності інформації, що забезпечує СІБ	max	max	max
9.	Середні витрати ресурсів СІБ та системою атаки	min	min	min
10.	Надійність функціонування СІБ	max	max	max
11.	Ефективність СІБ	max	max	max

На першому кроці виділимо рівні ієрархії частинних критеріїв та побудуємо їх структурну схему (рис. 1).

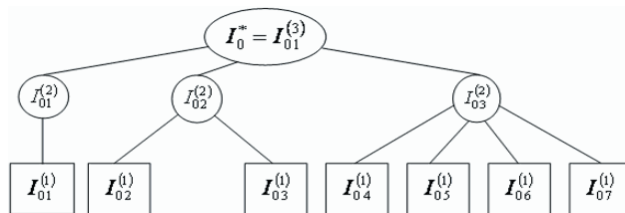


Рис. 1. Структурна схема ієрархії частинних критеріїв

На другому кроці нормування частинних критеріїв здійснимо згідно з (4) та викладеними рекомендаціями.

Так критерії першого рівня ієрархії $I_{01}^{(1)}, \dots, I_{07}^{(1)}$ (див. табл. 2 № з/п 1–7) подано у нормованому вигляді згідно з (4).

Результати оцінювання θ -ї властивості – ефективності СІБ на 3-му рівні ієрархії за заданими властивостями (див. табл. 2) одержані на третьому кроці, подано у табл. 3.

Їх аналіз показує, що найкращим варіантом побудови СІБ з можливих буде перший варіант – СІБ-1 (див. табл. 3), оскільки згідно з (5) СІБ-1 забезпечує найбільшу ефективність системи (3).

Висновки та перспективи подальших досліджень

Характерною перевагою розробленої технології багатокритерійного синтезу СІБ є науково обґрунтований підхід до оцінювання ефективності системи за відсутності обмежень на походження та кількість частинних критеріїв.

Це дозволяє у рамках багатокритерійного синтезу СІБ, що досліджується, оперувати значною сукупністю різних показників ефективності системи, цим самим сприяючи підвищенню адекватності СІБ реальним умовам її експлуатації.

У перспективі планується апробація запропонованої технології на СІБ введених в експлуатацію, з метою співставлення одержаних оцінок з реальними показниками ефективності системи.

Таблиця 3

Результати оцінювання

СІБ-1	Критерії 1-го рівня ієрархії						
	$I_{01}^{(1)}$	$I_{02}^{(1)}$	$I_{03}^{(1)}$	$I_{04}^{(1)}$	$I_{05}^{(1)}$	$I_{06}^{(1)}$	$I_{07}^{(1)}$
	0,66	0,5251	0,9645	0,0027	0,0328	0,0328	1
	Критерії 2-го рівня ієрархії						
	$I_{01}^{(1)}$		$I_{02}^{(1)}$		$I_{03}^{(1)}$		
	0,34		0,34		0,93		
	Критерії 3-го рівня ієрархії						
	$I_0^{(3)}$						
	0,28						
	Ефективність						
Достатньо ефективна							

СІБ-2	Критерії 1-го рівня ієрархії						
	$I_{01}^{(1)}$	$I_{02}^{(1)}$	$I_{03}^{(1)}$	$I_{04}^{(1)}$	$I_{05}^{(1)}$	$I_{06}^{(1)}$	$I_{07}^{(1)}$
	0,68	0,7325	0,9	0,0027	0,328	0,328	1
	Критерії 2-го рівня ієрархії						
	$I_{01}^{(1)}$			$I_{02}^{(1)}$		$I_{03}^{(1)}$	
	0,32			0,58		0,51	
	Критерії 3-го рівня ієрархії						
	$I_0^{(3)}$						
	0,49						
	Ефективність						
Ефективна							
СІБ-3	Критерії 1-го рівня ієрархії						
	$I_{01}^{(1)}$	$I_{02}^{(1)}$	$I_{03}^{(1)}$	$I_{04}^{(1)}$	$I_{05}^{(1)}$	$I_{06}^{(1)}$	$I_{07}^{(1)}$
	0,9	0,2514	0,2514	0,0027	0,028	0,0328	1
	Критерії 2-го рівня ієрархії						
	$I_{01}^{(1)}$			$I_{02}^{(1)}$		$I_{03}^{(1)}$	
	0,1			0,62		0,99	
	Критерії 3-го рівня ієрархії						
	$I_0^{(3)}$						
	0,37						
	Ефективність						
Достатньо ефективна							

Література

1. Попова Е.А. Об использовании методов многокритериального поиска в сфере информационной безопасности / Е. А. Попова // Вестник АГТУ.: Сер.: Управление, вычислительная техника и информатика. – Астрахань: АГТУ, 2010. – № 1. – С. 67-72.
2. Ленков С.В. Методы и средства защиты информации : монография [в 2-х т.] Т. 2. Информационная безопасность / С. В.Ленков, Д. А.Перегулов, В. А. Хорошко. – К.: Арий, 2008. – 344 с.
3. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации / А. А. Малюк. – М.: Горячая линия – Телеком, 2004. – 280 с.
4. Домарев В. В. Безопасность информационных технологий. Системный подход / В. В. Домарев. – К.: Диасофт, 2004. – 992 с.
5. Иванченко Е. В. Методология синтеза систем анализа и оценки рисков потерь информационных ресурсов / Е. В. Иванченко, С. В. Казмирчук, А. Ю. Гололобов // Захист інформації. – К.: НАУ, 2012. – № 2. – С. 5-9.
6. Тимошенко А. О. Синтез систем захисту інформації з використанням логіки імовірнісних методів: автореф. дис. на здобуття наук. ступеня канд. тех. наук : спец. 05.13.21 “Сист. зах. інф.” / А. О. Тимошенко. – К., 2002. – 15 с.
7. Маслова Н. А. Методы оценки эффективности систем защиты информационных систем / Н. А. Маслова // Штучний інтелект. – Донецьк: ІШП, 2008. – № 4. – С. 253-264.
8. Гарасимчук О. І. Оцінка ефективності систем захисту інформації / О. І. Гарасимчук, Ю. М. Костів // Вісник КНУ ім. М. Остроградського. – Кременчук: КНУ ім. М. Остроградського, 2011. – № 1 (66). – С. 16-20.
9. Новіков О. М. Оптимальний синтез параметрів системи захисту інформації / О. М. Новіков, А. М. Родіонов, А. О. Тимошенко // Наукові вісті НТУУ “КПІ”. – К.: НТУУ “КПІ”, 2007. – № 4. – С. 146-151.
10. Воронин А. Н. Многокритериальные решения: модели и методы: монография / А. Н. Воронин, Ю. К. Зиятдинов, М. В. Ку克林ский. – К.: НАУ, 2011. – 348 с.
11. Гришук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : монографія / Р. В. Гришук. – Житомир: Рута, 2010. – 280 с.

Abstract

The dynamic development of information security sphere are constantly brings new demands to the respective information security systems. As a rule, a record of all such requirements is connected with the problem of multicriteria optimization, which is aggravated by weakly formalized requirements. They are of different physical dimension and quantitative and qualitative measurement, and they have contradictory nature that limits the application field of the existing methods of multicriteria optimization.

The article represents the modern technology of multicriteria synthesis of information security systems, based on the inserted scalar folding technique, adapted to the solution of a particular issue. The application of suggested technology allows taking into account the variety of requirements to the information security system, as well as removes the issue of their amount and nature of origin. As a result of multicriteria synthesis of information security system, according to the suggested technology, the designer of the system has an opportunity to assess the level of information security, which the system will be able to provide.

The article presents a model example of application of the suggested methodology

Keywords: information security system, scalar folding, optimization criterion, multicriteria synthesis, technology

В результаті проведеного аналізу робіт визначена необхідність розробки джерел для виміру і контролю діелектричної проникності біологічних об'єктів. Проведено визначення наближеної формули, яка зв'язує резонансну частоту з геометричними і електродинамічними параметрами резонатора. Були досліджені коливання «шепучої галереї». Основна увага приділена вивченню залежності резонансних частот і радіаційних добротностей від зміни товщини резонатора

Ключові слова: резонатор, частота, коливання, добротність, спектр, об'єкт, джерело

В результате проведенного анализа работ определена необходимость разработки источников для измерения и контроля диэлектрической проницаемости биологических объектов. Проведено определение приближенной формулы, которая связывает резонансную частоту с геометрическими и электродинамическими параметрами резонатора. Были исследованы колебания «шепчущей галереи». Основное внимание уделено изучению зависимости резонансных частот и радиационных добротностей от изменения толщины резонатора

Ключевые слова: резонатор, частота, колебание, добротность, спектр, объект, источник

УДК 614.89:537.868

ОПРЕДЕЛЕНИЕ ЗАВИСИМОСТЕЙ ДЛЯ СОБСТВЕННЫХ ЧАСТОТ РЕЗОНАТОРА

Н. П. Кунденко

Кандидат технических наук, доцент

Кафедра «Интегрированные
электротехнологии и процессы»

Харьковский национальный технический
университет сельского хозяйства

им. П. Василенко

ул. Артема, 44, г. Харьков, Украина, 61002

Контактный тел.: (057) 712-28-33

E-mail: n.p.kundenko@inbox.ru

1. Введение

Проведенный анализ работ показал, что точность измерений ДП зависит от стабильности частоты генератора и добротности измерительного резонатора. Аппаратура, предназначенная для измерения изменений диэлектрических параметров жидкости,

должна обеспечивать не только необходимый уровень подводимой мощности и частоты сигнала, но и удовлетворять высоким требованиям по стабильности частоты, степени подавления дискретных составляющих в спектре выходного сигнала, габаритам, надежности, экономичности и сроку службы. Результаты численного анализа показывают, что для