УДК 004.681

ОПТИМІЗАЦІЙНІ ЕКОНОМІЧНІ ЗАДАЧІ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Є.Г. ЛЕВЧЕНКО, Р.Б. ПРУС

Розроблено математичну модель і методику визначення оптимального розподілу ресурсів між об'єктами захисту інформації. Сформульовано цільову функцію, на основі якої проведено ілюстративні розрахунки в системі з двох інформаційних об'єктів. Окреслено напрямки розвитку запропонованої методики.

ВСТУП

Математичне моделювання економічних задач часто призводить до необхідності оптимізації функції, яка містить певні показники. У задачах інформаційної безпеки ця функція частіше за все характеризує втрати інформації, які необхідно мінімізувати при деяких обмеженнях, що накладаються на параметри розрахунку (наприклад, витрати на захист інформації). І функція, і обмеження можуть мати як лінійний, так і нелінійний характер, обмеження накладаються у вигляді рівнянь або нерівностей [1, 2].

Розглянемо одну з актуальних задач менеджменту інформаційної безпеки — оптимізацію розподілу ресурсів між об'єктами захисту інформації [3, 7]. Цільова функція цієї задачі, яка визначає втрати інформації, у загальних рисах має такий вигляд:

$$i(x,y)=\sum_{k=1}^{l} i_k =\sum_{k=1}^{l} g_k p_k q_k(x) f_k(x,y), \qquad (1)$$

де x та y — ресурси нападу і, відповідно, захисту; g — об'єм інформації на об'єкті; p — імовірність нападу на певний об'єкт; $q(x)$ — імовірність виділення нападом ресурсів x для вилучення інформації з об'єкта; $f(x,y)$ — залежність частки вилученої інформації від ресурсів x та y.

Обмеження накладаються на x та y: $\sum_k x_k = X$, $\sum_k y_k = Y$, $k=\overline{1,l}$ — номер об'єкта.

Оптимізація функції $f(x,y)$ ведеться по одній із змінних — x або y друга змінна при цьому вважається константою. Цю задачу можна

розв'язати аналітично — методом Якобі або методом множників Лагранжа, а у випадку двох змінних ($k=\overline{1,2}$, $\{x\}=x_1,x_2$) і графічно [1].

Основні труднощі, які виникають під час розв'язання поставленої задачі, полягають у побудові математичної моделі. Цю проблему при обраному виді цільової функції можна поділити на дві частини: вибір залежності $f_k(x,y)$, $q_k(x)$ і визначення параметрів розрахунку g_k, p_k для кожного об'єкта.

Під час вибору залежності $f(x,y)$ слід врахувати, що вона має задовольняти двом умовам: при $x\to 0$ $f(x,y)\to 0$, при $x/y>>1$ $f(x)$ асимптотично прямує до 1. Цим умовам відповідають функції виду $f(x)=$ $=\dfrac{ax^{2n}}{bx^{2n}+c}$ і $f(x)=1-de^{-mx}$. У цих виразах і в подальшому вважатимемо, що $y=1$. Константи a, b, c, d, n, m, які визначають положення та нахил кривих, можуть бути встановлені шляхом «прив'язки» до характерних точок. За нестачі статистичної інформації прив'язку можна здійснити шляхом логічних міркувань на основі експертної оцінки. Вважатимемо, що при $x=1$ $f(x)\approx 0{,}5$. Тоді найбільш придатними будуть функції, зображені на рис. 1 (крива *1* — $f=\dfrac{x}{1+x}$, крива *2* — $f=\dfrac{x^2}{1+x^2}$, крива *3* — $f=1-e^{x^2}$).

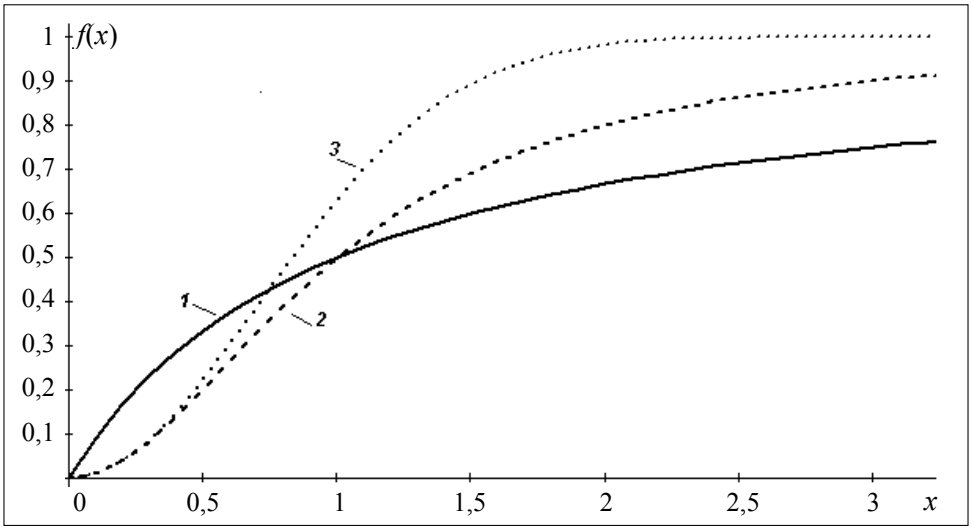

Рис. 1. Залежності кількості вилученої інформації від ресурсів нападу

Аналіз протистояння сторін почнемо з системи, яка складається з двох інформаційних об'єктів. Залежність $f(x)$ оберемо у вигляді $f(x)=\dfrac{x}{1+x}$. Тоді цільова функція матиме вигляд:

$$i(x_1,x_2)=g_1\frac{x_1}{1+x_1}+g_2\frac{x_2}{1+x_2}. \qquad (2)$$

У цьому виразі для спрощення аналізу прийнято, що $p=1$, $q=\text{const}$, тобто вважаємо, що ймовірності нападу однакові для об'єктів $k=\overline{1,2}$ та ін-

тервалу $X \in [0,3]$, в якому проводиться дослідження. Величини g_k нормовані: $g_1 + g_2 = 1$.

Оптимальне значення цільової функції $i(x_1, x_2) \to \max$ (для функції $i(y)$ оптимумом, очевидно, буде $i(y_1, y_2) \to \min$) досягається в точці дотику лінії рівня $i(x_1, x_2) = C = \text{const}$, яка визначає кількість інформації, вилученої з обох об'єктів при різних варіантах розподілу ресурсів нападу між об'єктами, і обмежувальної прямої $H(x) = x_1 + x_2 = X$, яка визначається загальною величиною ресурсів нападу.

Залежність $i(x_1, x_2)$ зображено на рис. 2 (крива *1* — на першому об'єкті, крива *2* — на другому об'єкті). Фізичний зміст ця фігура має в площині $x_1 0 x_2$ (на рисунку зображена суцільною лінією).

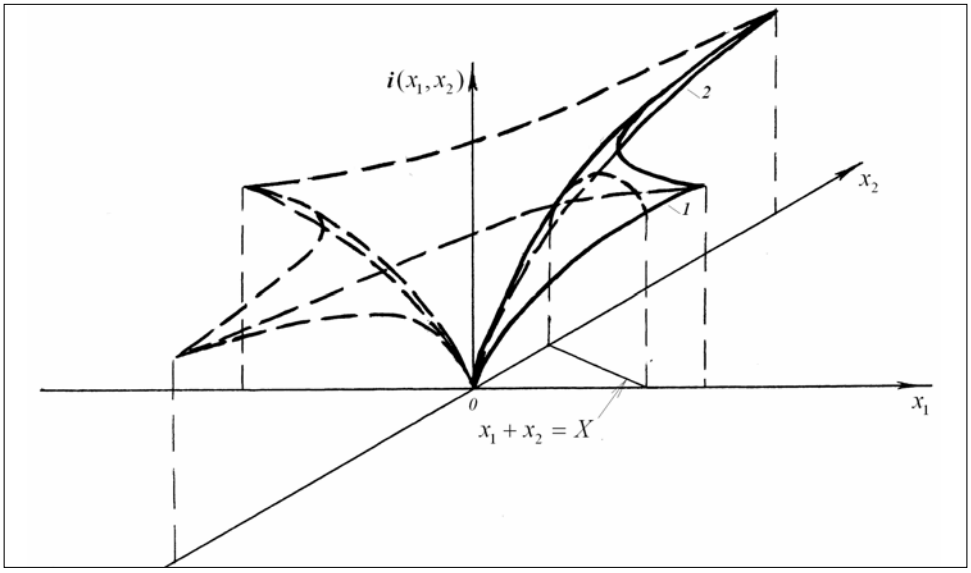

Рис. 2. Залежність кількості вилученої інформації від розподілу ресурсів нападу між об'єктами

Нахил кривих 1 і 2 на рис. 2 залежить не лише від значень x_1 та x_2, а й від обсягів інформації g_1 та g_2, оскільки кількість вилученої інформації з об'єкта, на якому обсяг інформації менший, зростатиме повільніше по відношенню до вкладених ресурсів нападу (рис. 3).

Лінії рівня $i(x_1, x_2) = g_1 \dfrac{x_1}{1 + x_1} + g_2 \dfrac{x_2}{1 + x_2} = C$ отримуємо в результаті перерізу просторової фігури, зображеної на рис. 2 площинами, паралельними площині $x_1 0 x_2$.

Досягти дотику кривої $i(x_1, x_2) = C$ і прямої $H(x)$ можна двома шляхами. Якщо в умові задано кількість ресурсів X, тобто положення прямої $H(x)$, то необхідно рухати лінію рівня $i(x_1, x_2) = C$ у напрямку прямої $H(x)$ до досягнення дотику. Точка дотику буде визначати максимальну кількість інформації, яка може бути вилучена при заданому значенні X. Якщо ж ставиться задача визначення необхідної кількості ресурсів для вилучення певної кількості інформації (вона задається кривою $i(x_1, x_2) = C$), то

лінія рівня залишається нерухомою, а пряму $H(x)$ слід рухати в напрямку кривої $i(x_1, x_2) = C$, і при дотику визначити величину необхідних ресурсів X.

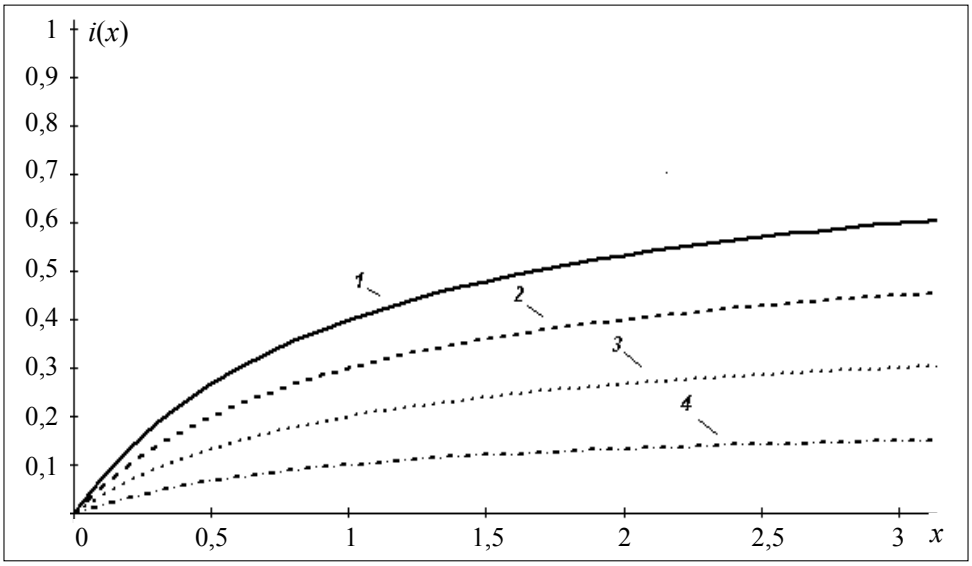

Рис. 3. Залежність кількості вилученої інформації від ресурсів нападу при різних значеннях g: крива *1* — $g = 0{,}8$; крива *2* — $g = 0{,}6$; крива *3* — $g = 0{,}4$; крива *4* — $g = 0{,}2$

На рис. 4 зображено оптимальні розв'язки при обмеженні $X = x_1 + x_2 = 1$ залежно від обсягу інформації g_1 та g_2 на об'єктах. Цифрами позначено: крива *1* — $H(x) = x_1 + x_2 = 1$; крива *2* — $\frac{g_1}{g_2} = \frac{0{,}5}{0{,}5} = 1$, $i(x_1, x_2) = 0{,}33$; крива *3* — $\frac{g_1}{g_2} = \frac{0{,}6}{0{,}4} = 1{,}5$, $i(x_1, x_2) = 0{,}34$; крива *4* — $\frac{g_1}{g_2} = \frac{0{,}7}{0{,}3} = 2{,}33$, $i(x_1, x_2) = 0{,}362$; крива *5* — $\frac{g_1}{g_2} = \frac{0{,}8}{0{,}2} = 4$, $i(x_1, x_2) = 0{,}4$.

Із рис. 4 видно, що оптимальне значення $i(x_1, x_2)$ для $\frac{g_1}{g_2} = \frac{0{,}8}{0{,}2}$ досягається при $x_1^0 = 1$ та $x_2^0 = 0$, і як видно з (2), становить 0,4.

Перейдемо до аналітичних методів розв'язку поставленої задачі. Перший з них — метод Якобі у випадку двох змінних дозволяє, використовуючи обмежувальне рівняння $x_1 + x_2 = X$, звести задачу на умовний екстремум функції двох змінних до задачі на безумовний екстремум функції однієї змінної:

$$i(x_1) = g_1 \frac{x_1 / y_1}{1 + x_1 / y_1} + g_2 \frac{(X - x_1)/y_2}{1 + (X - x_1)/y_2}.$$

Умовою оптимальності є $\frac{di(x_1)}{dx_1} = 0$. Проте пошук значення x_1^0 призводить до необхідності розв'язку алгебраїчного рівняння високого ступеня. Таким чином, навіть у випадку двох об'єктів цей метод призводить до

досить громіздкої обчислювальної процедури. Звертаючись до другого з аналітичних методів, методу множників Лагранжа, будуємо функцію:

$$L(x_1, x_2, \lambda) = g_1 \frac{x_1/y_1}{1 + x_1/y_1} + g_2 \frac{x_2/y_2}{1 + x_2/y_2} + \lambda (x_1 + x_2 - X). \qquad (3)$$

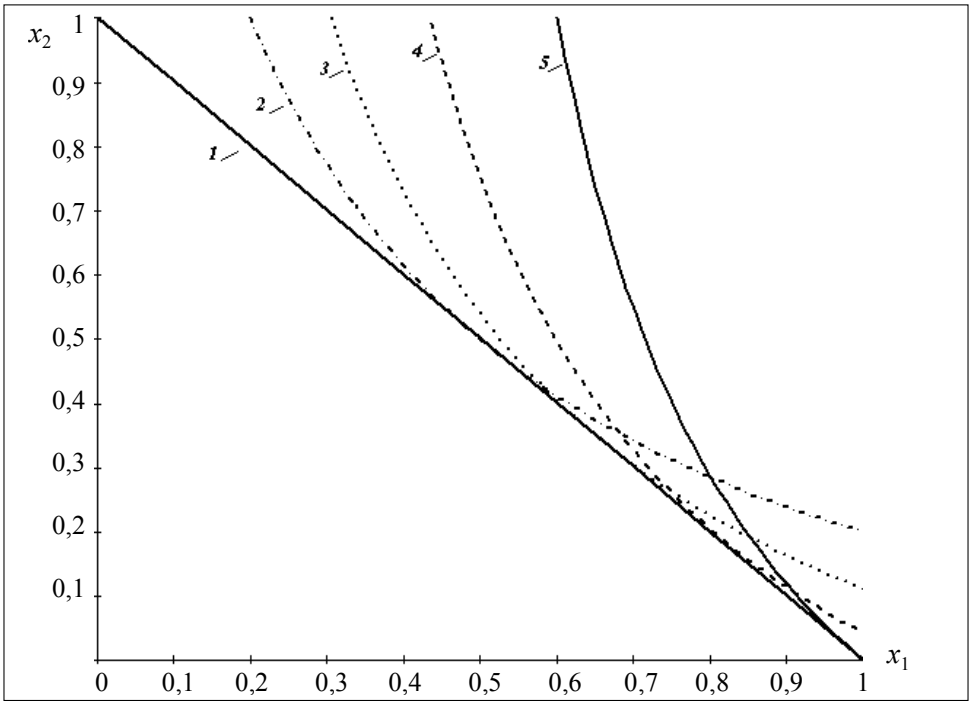

Рис. 4. Геометрична інтерпретація досягнення оптимуму в системі з двох об'єктів захисту інформації при різних значеннях g_1, g_2

Прирівнюючи перші похідні до нуля $\frac{\partial L}{\partial x_1} = 0$; $\frac{\partial L}{\partial x_2} = 0$; $\frac{\partial L}{\partial \lambda} = 0$, отримуємо оптимальні значення

$$x_1^0 = \sqrt{\frac{g_1 y_1}{\lambda}} - y_1,\ x_2^0 = X - x_1^0,\ \lambda = \frac{(\sqrt{g_1 y_1} + \sqrt{g_2 y_2})^2}{(X + y_1 + y_2)^2}.$$

Користуючись даними про обсяг інформації на об'єктах, захист має змогу визначити оптимальний розподіл ресурсів нападу, за якого можливе вилучення максимальної кількості інформації при різних значеннях g_1 та g_2. На основі отриманих результатів захист приймає рішення про розподіл власних ресурсів з метою протидії нападу.

Оптимальний розподіл ресурсів захисту можна знайти також прямим шляхом, прирівнюючи похідні функції (3) до нуля: $\frac{\partial L}{\partial y_1} = 0$; $\frac{\partial L}{\partial y_2} = 0$; $\frac{\partial L}{\partial \lambda} = 0$. Оптимальні значення y_1^0 і y_2^0 розраховуємо за виразами:

$$y_1^0 = -x_1 + \sqrt{\frac{g_1 x_1}{|\lambda|}} \text{ та } y_2^0 = -x_2 + \sqrt{\frac{g_2 x_2}{|\lambda|}},\ \lambda = -\frac{\left(\sqrt{g_1 x_1} + \sqrt{g_2 x_2}\right)^2}{(X + Y)^2}.$$

У випадку, коли кількість об'єктів перевищує два, оптимальний розподіл ресурсів захисту знаходимо за формулою:

$$y_k = -x_k + \sqrt{\frac{g_k x_k}{|\lambda|}}, \text{ де } \lambda = -\frac{\left(\sum_{k=1}^{l} \sqrt{g_k x_k}\right)^2}{(X+Y)^2}.$$

ВИСНОВКИ

Проведені розрахунки показують, що оптимальний розподіл ресурсів як захисту, так і нападу фактично повторює співвідношення $g_1 : g_2$. Межі справедливості цього висновку може бути встановлено після проведення більш детальних досліджень із уточненням залежності $f(x, y)$.

Викладена методика може мати продовження в таких напрямах:

1. Ускладнення математичної моделі шляхом задання різних функцій $f_k(x, y)$ для кожного k-го об'єкта — відображення різного степеня вразливості об'єктів, яка визначається рівнем їх природної та технічної захищеності.
2. Перехід до стохастичної задачі, коли параметри розрахунків g_k, p_k, $g_k(x)$ і форми залежностей $f_k(x, y)$ задаються за результатами їх експертної оцінки.
3. Двохетапний розв'язок поставленої задачі: перший етап — розвідка, другий — здобуття інформації; у цьому випадку оптимізації підлягає також розподіл ресурсів між етапами.
4. Аналіз комплексного протистояння двох сторін, коли кожна зі сторін розподіляє свої ресурси на два канали: захист своєї інформації та здобуття інформації про конкурента.
5. Розробка оптимального управління системою інформаційної безпеки — синтез оптимальних систем.

ЛІТЕРАТУРА

1. *Вентцель Е.С.* Исследование операций. — М.: Советское радио, 1972. — 552 с.
2. *Таха Х.* Введение в исследование операций. — М.: Вильямс, 2005. — 912 с.
3. *Левченко Є.Г.* Оптимізація розподілу ресурсів між об'єктами захисту інформації // НТЖ «Захист інформації». — 2007. — № 1. — С. 33–38.
4. *Олексюк О.С.* Проблеми фінансування витрат на захист інформації в економічній діяльності // Праці Міжнародного Симпозіуму «Питання оптимізації обчислень». — 2009. — Т. 2. — С. 170–172.
5. *Задірака В.К., Олексюк О.С., Смоленюк Р.П., Штабалюк П.І.* Фінансування витрат на захист інформації в економічній діяльності // Університетські наукові записки. — 2006. — № 3–4 (19–20). — С. 479–490.
6. *Gordon L., Loeb M.* The Economics of Information Security Investment // ACM Transactions on Information and System Security, November 2002. — **5**, № 4. — P. 438–457.
7. *Liu W.*, *Tanaka H., Matsuura K.* Empirical-Analysis Methodology for Information-Security Investment and it's Application to Reliable Survey of Japanese Firms // IPSJ Journal, September 2007. — **48**, № 9. — P. 3204–3218.

Надійшла 29.06.2009