УДК 004.681

Демчишин М.В. (НАУ)

ГЕОМЕТРИЧНА ІНТЕРПРЕТАЦІЯ ОПТИМІЗАЦІЇ РОЗПОДІЛУ РЕСУРСІВ МІЖ ОБ'ЄКТАМИ ЗАХИСТУ ІНФОРМАЦІЇ

Розглянуті пряма і зворотна оптимізаційні задачі розподілу ресурсів при протистоянні двох сторін. Проаналізоване положення критичних точок, які відображають зміну стратегії в розподілі ресурсів. Приведена методика може бути використана при розробці алгоритму динамічного управління ресурсами захисту інформації.

Ключові слова: інформаційна безпека, розподіл ресурсів, критичні точки.

Вступ. Важливим напрямком економічного менеджменту інформаційної безпеки є визначення оптимального розміру ресурсів захисту і їх розподілу між об'єктами [1-4]. У випадку двох об'єктів розв'язок можна подати в геометричній формі. Не дивлячись на обмеження в кількості об'єктів, такий підхід викликає інтерес, оскільки дозволяє наочно продемонструвати методику пошуку оптимуму і його залежність від параметрів математичної моделі.

Мета роботи – проілюструвати методику визначення оптимальної кількості ресурсів і їх розподілу між об'єктами в умовах протистояння двох сторін в інформаційній сфері.

Результати досліджень. В умовах невизначеності при пошуку оптимального рішення слід передбачити всі можливі варіанти дій суперника, в тому числі найбільш несприятливий для нас і оптимальний для суперника. Проте при пошуку такого варіанта суперник знаходиться в такому ж стані невизначеності і зазнає таких же труднощів. В результаті ми приходимо до необхідності розв'язку двоїстої задачі шляхом рекурентних процедур, тобто почергового пошуку оптимуму кожної з сторін при прогнозованій стратегії суперника. В термінології теорії ігор це позиційна гра.

Проілюструємо цю методику на прикладі. Розглянемо спочатку дії нападу і використаємо цільову функцію у вигляді [4]:

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

де $i(x,y)$ – частка вилученої інформації;

x і y – змінні величини, які визначають ресурси нападу і, відповідно, захисту;

g_k – відносна кількість інформації на k-му об'єкті;

$p_k(x,y)$ – імовірність нападу на k-й об'єкт;

$q_k(x,y)$ – імовірність виділення нападом ресурсів x на k-ий об'єкт;

$f_k(x,y)$ – залежність частки вилученої інформації на k-му об'єкті від співвідношення x та y.

Зазначимо, що за браком статистичних даних величини, які стоять в правій частині (1) задаються евристично або визначаються шляхом експертної оцінки.

На першому кроці розглянемо дії нападу. При цьому оптимізаційна задача формулюється так:

$$i(x,y)\to\max, \qquad (2)$$

де $x\ge 0,\ y\ge 0,\ \sum_{k=1}^{l} x_k = x,\ \sum_{k=1}^{l} y_k = y$.

У подальшому x і y позначають сумарні ресурси нападу і захисту, а в функціональних залежностях – незалежні змінні.

Маючи на меті геометричну інтерпретацію розв'язку, розглянемо систему з двох об'єктів. Враховуючи, що складові цільової функції визначаються відношенням x/y, введемо нову змінну $\tilde{x} = x/y$. Цільова функція при цьому приймає вигляд:

$$i(\tilde{x}) = \sum_{k=1}^{l} g_k \cdot p_k(\tilde{x}) \cdot q_k(\tilde{x}) \cdot f_k(\tilde{x}),$$

де $\tilde{x} = x/y$. У нашому розгляді x і y перестають бути незалежними змінними і змінюються під дією протилежної сторони. Оберемо залежності $f(\tilde{x})$ у вигляді [4]: $f(\tilde{x}) = \frac{\tilde{x}^n}{\tilde{x}^n + c}$, де параметри n і c визначають положення і крутизну кривої на різних ділянках. Зокрема, при n=1 опуклість кривої $f(\tilde{x})$ направлена догори, при n>1 – донизу. При збільшенні c крива опускається вниз, причому вплив цього параметру проявляється в більшій степені в початковій області – при $\tilde{x} \lesssim 1$. Прагнучи відобразити особливості залежностей $f(\tilde{x})$, розглянемо функції з різними значеннями n і c:

$$f(\tilde{x}) = \frac{\tilde{x}}{\tilde{x} + 4} \quad (3) \quad f(\tilde{x}) = \frac{\tilde{x}^2}{\tilde{x}^2 + 16} \quad (4) \quad f(\tilde{x}) = \frac{\tilde{x}^3}{\tilde{x}^3 + 32} \quad (5) \quad f(\tilde{x}) = \frac{\tilde{x}^4}{\tilde{x}^4 + 64}. \quad (6)$$

У подальших розрахунках будемо обирати залежності $f(\tilde{x})$ для двох об'єктів у вигляді пар з приведеного набору (3-6).

Розглянемо спрощений варіант, в якому $q(\tilde{x}) = const$. З нормовочної умови $\int_0^{\tilde{x}_{гр}} q(\tilde{x}) d\tilde{x} = 1$, де $x_{гр}$ обмежує інтервал можливих значень $\tilde{x}$, при обраному $x_{гр} = 3$ одержуємо $q = \frac{1}{3}$. Розглянемо два варіанта вибору залежностей $f_k(\tilde{x})$ для системи з двох об'єктів: функції (3), (5) (рис. 1) і функції (4), (6) (рис. 2).

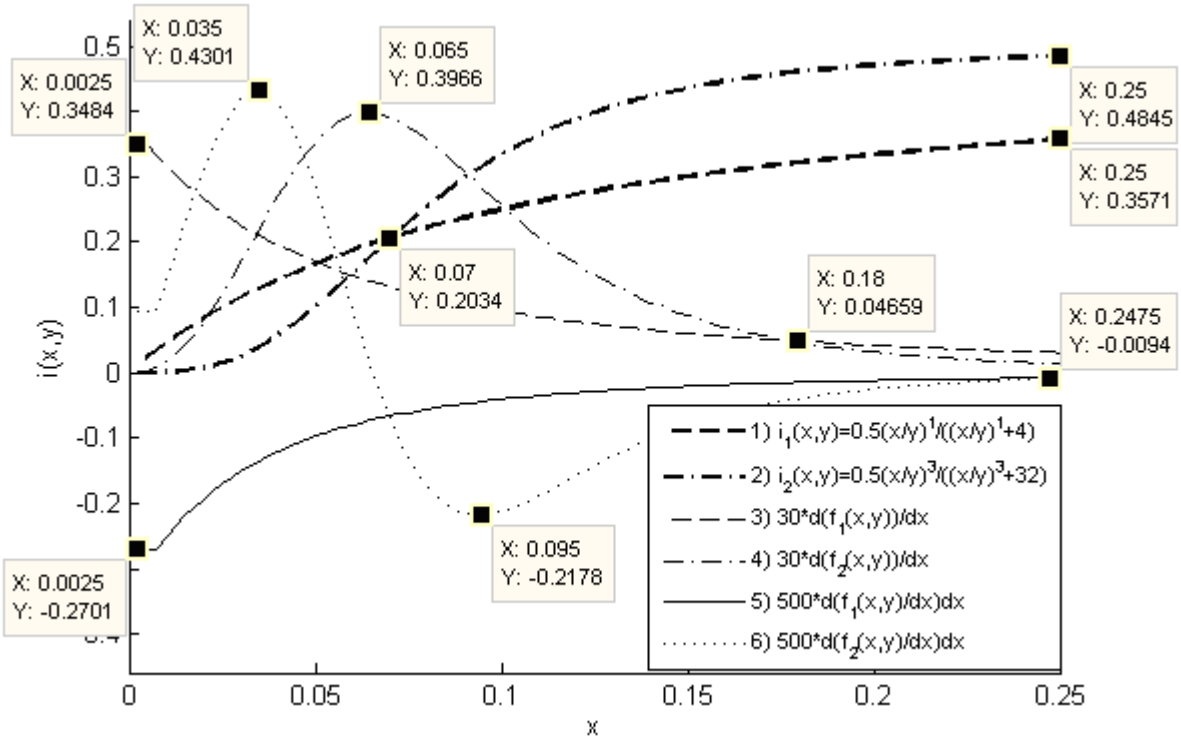

Рис. 1. Залежності $i(\tilde{x})$ та похідні від них, одержані на основі дробно-лінійної (3) і дробно-нелінійної (5) функцій $f(\tilde{x})$

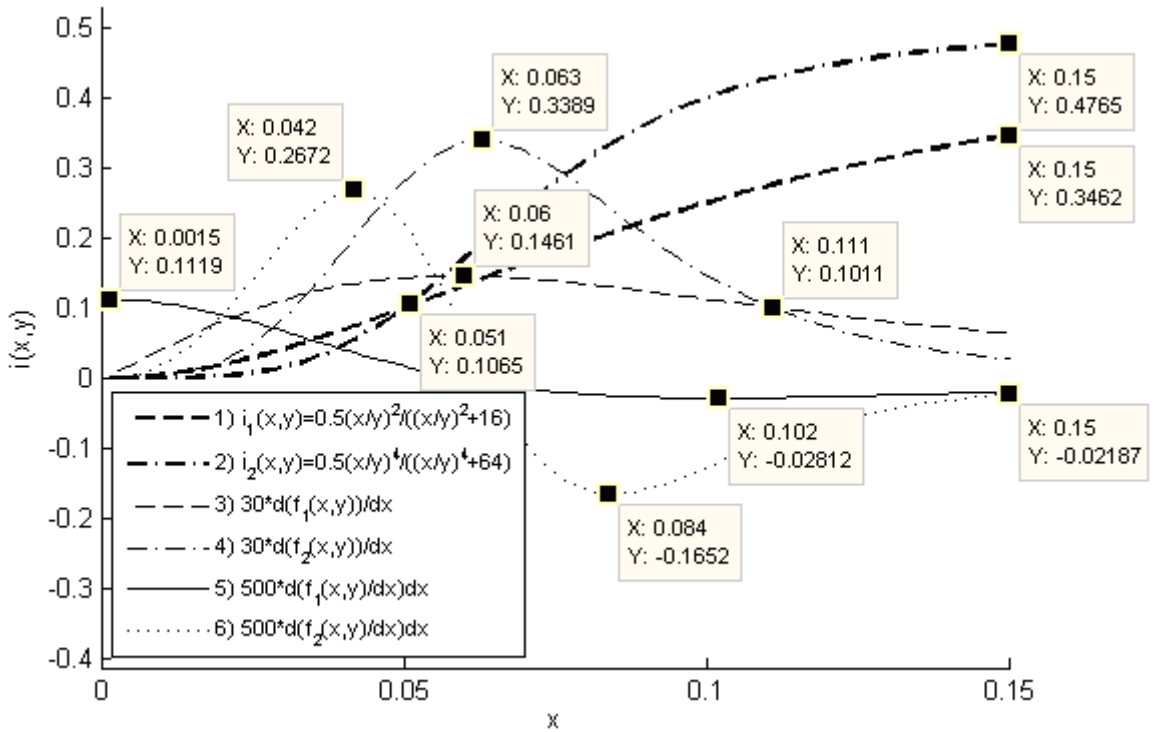

Рис. 2. Залежності $i(\tilde{x})$ та похідні від них, одержані на основі дробно-нелінійних функцій (4) і (6)

Припустимо також $g_1 = g_2 = 0{,}5$, $p_1(\tilde{x}) = p_2(\tilde{x}) = 1$ і одержимо:

1) для першого варіанту

$$i(\tilde{x}) = i_1(\tilde{x}) + i_2(\tilde{x}) = \frac{1}{2}\frac{1}{3}\left(\frac{\tilde{x}}{\tilde{x}+4} + \frac{\tilde{x}^3}{\tilde{x}^3+32}\right). \quad (7)$$

2) і для другого

$$i(\tilde{x}) = i_1(\tilde{x}) + i_2(\tilde{x}) = \frac{1}{2}\frac{1}{3}\left(\frac{\tilde{x}}{\tilde{x}+16} + \frac{\tilde{x}^4}{\tilde{x}^4+64}\right). \quad (8)$$

Ці залежності, а також перші та другі похідні залежностей $f(\tilde{x})$, приведені з масштабними коефіцієнтами 30 і , відповідно, 500, зображені на рис. 1,2. Квадратиками позначені екстремальні значення функцій.

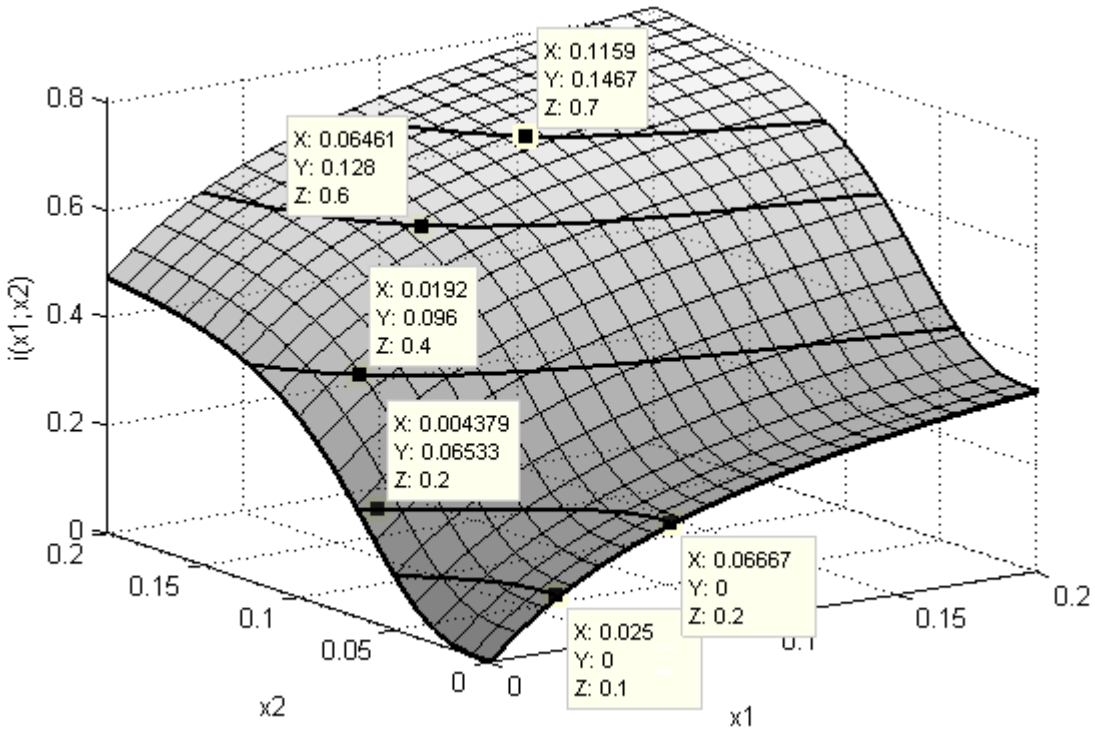

Рис. 3. Залежність частки вилученої інформації від ресурсів нападу на двох об'єктах

Цільова функція $i(x_1, x_2)$ в геометричній інтерпретації зображується у вигляді просторової фігури в системі координат x_1, x_2, де x_1 і x_2 – ресурси нападу, направлені на кожний з двох об'єктів (ресурси захисту y_1 і y_2 вважаються відомими і при розрахунках виступають в ролі параметрів). Фігура побудована на функціях $i_1(x, y)$ і $i_2(x, y)$ (рис. 3). При побудові фігури (рис.3) задані такі значення параметрів: $g_1 = g_2 = 0{,}5$, $y_1 = y_2 = 0{,}025$.

Аналізуючи дії кожної з сторін, будемо розрізняти два типи задач – пряму і зворотну. В першому випадку задають кількість ресурсів (нападу і, відповідно, захисту) і визначають їх розподіл по об'єктах, який забезпечує досягнення оптимального значення цільової функції (максимального і, відповідно, мінімального). При рішенні зворотної задачі задається значення цільової функції і потрібно знайти оптимальні значення необхідних ресурсів і їх розподіл по об'єктах. Геометричний розв'язок прямої задачі одержуємо в результаті перерізу просторової фігури $i(x_1, x_2)$ вертикальною площиною, яка проходить через обмежувальну пряму $x = x_1 + x_2 = C$, розв'язок зворотної – в результаті перерізу цієї фігури горизонтальною площиною, розташованою на рівні заданого значення *i* (рис. 3). В першому випадку оптимум знаходиться в найвищій точці перерізу, в другому – в точці дотику кривої,

одержаної в результаті перерізу, до прямої $x_1 + x_2 = x = C$, яка визначає необхідну для досягнення заданого значення *i* кількість ресурсів (рис. 4, жирні криві).

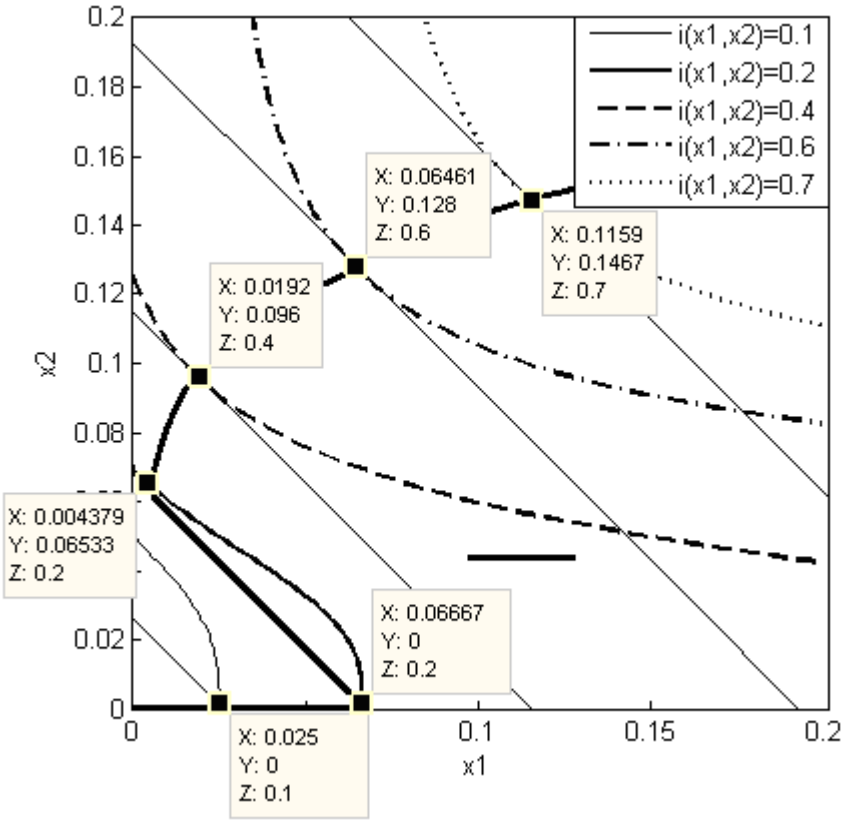

Рис. 4. Лінії перерізу просторової фігури (рис. 3) на різних рівнях

Положення оптимальних точок (вони зображені квадратиками) дозволяє визначити необхідну кількість ресурсів x – вона визначається діагональною прямою $x = const$, яка є дотичною до кривої перерізу, а відстань між сусідніми прямими характеризує темп зростання x при збільшенні $i(x)$. На цьому ж рисунку показано положення критичної точки, при досягненні якої слід переходити від зосередження ресурсів нападу на одному об'єкті до їх розподілу між обома об'єктами (на рис. 4 $x_{кр} = 0.067$, а $i_{кр} = 0.2$).

Лінія яка з'єднує оптимальні точки, є результат розрахунків зворотної задачі, в якій по заданим значенням $i(x_1, x_2)$ знаходять оптимальні значення x_1^0, x_2^0, x^0. Ці лінії зображені на рис. 5-7, в яких використані різні залежності $f_k(x, y)$. Розв'язки оптимізаційних задач одержано з допомогою пакету Optimization Toolbox програмного комплексу Matlab.

При аналізі залежностей (рис. 5-7) нас в першу чергу цікавить положення критичних точок, які відображають зміну стратегії в розподілі ресурсів. Перші дві з них – $x_{кр1}$ і $x_{кр2}$ визначають перехід від концентрації ресурсів на одному з об'єктів до їх зосередження на іншому ($x_{кр1}$) або до розподілу між обома об'єктами ($x_{кр2}$) (рис. 6). Третя характерна точка відображає не зміну стратегії, а відображає лише якісну зміну переваги в розподілі ресурсів від одного об'єкта до іншого (для однотипності позначимо її через $x_{кр3}$). На рис. 5 $x_{кр1}$ відсутня, $x_{кр2} = 0{,}069$, $x_{кр3} = 0{,}356$; на рис. 6 $x_{кр1} = 0{,}049$, $x_{кр2} = 0{,}136$, $x_{кр3} = 0{,}215$.

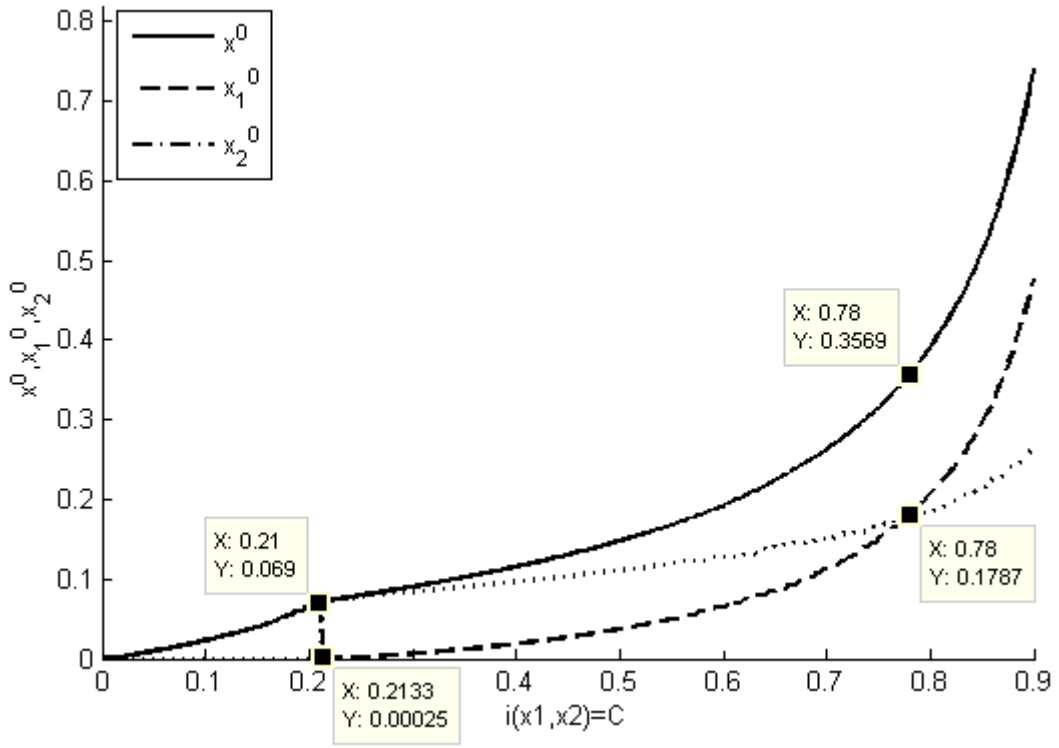

Рис. 5. Оптимальний розподіл ресурсів нападу між двома об'єктами, які характеризуються функціями (3), (5)

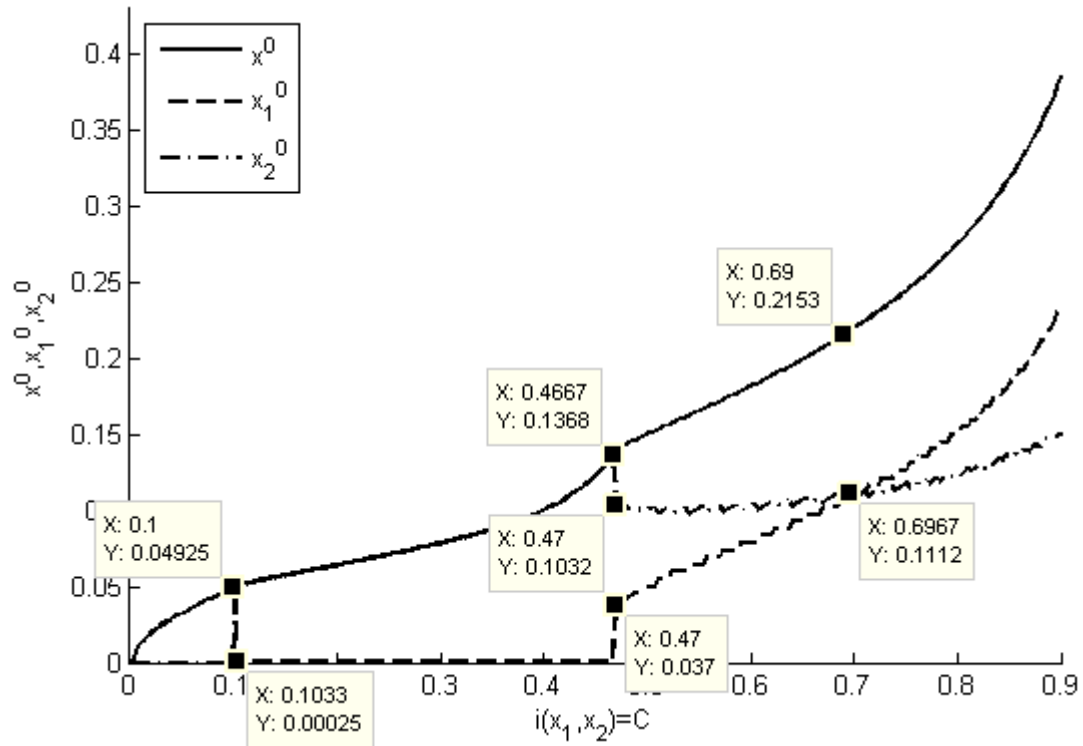

Рис. 6. Оптимальний розподіл ресурсів нападу між двома об'єктами, які характеризуються функціями (4), (6)

Вплив параметрів n і c в залежностях $f_k(x, y)$ на положення критичних точок можна сформулювати наступним чином.

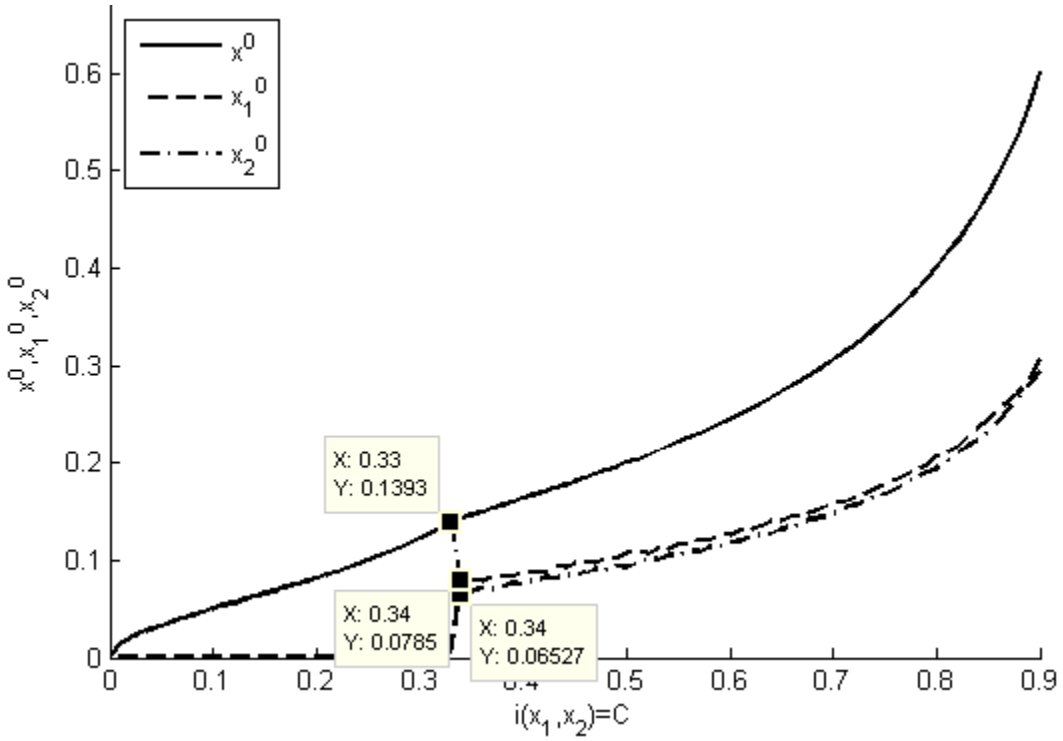

Рис. 7. Оптимальний розподіл ресурсів нападу між двома об'єктами з однаковими залежностями $f_k(x)$ (4)

1. При збільшенні n значення $x_{крі}$ ($i = 1,2,3$) зменшуються, $i_{кр1}$ та $i_{кр3}$ зменшуються, а $i_{кр2}$ зростають (рис. 5 і 6).

2. При збільшенні c і $n_1 \neq n_2$ $x_{крі}$ зростають, $i_{кр2}$ також зростає, а $i_{кр3}$ зменшується.

Отже, при збільшенні n і збільшенні c значення $x_{крі}$ змінюються різнонаправлено.

Положення критичних точок визначається кривизною функцій $f_1(\tilde{x})$ і $f_2(\tilde{x})$ та відображає перехід до нового принципу розподілу, який забезпечує більший приріст значень цільової функції при подальшому зростання x. Зокрема, при $x = x_{кр1}$ (рис. 3б) $f_1(x_{кр1}) + \frac{df_1}{dx_1}dx_1 = f_2(x_{кр1}) + \frac{df_2}{dx_2}dx_2$ і при подальшому зростанні x права частина рівності перевищує ліву. При переході через другу критичну точку $x_{кр2}$ значення x можна поділити на дві складові x_1 і x_2, $x_1 + x_2 = x$ – такі, що сума $f_1(x_1) + \frac{df_1}{dx_1}dx_1 + f_2(x_2) + \frac{df_2}{dx_2}dx_2$ стає більшою від кожної з величин $f_1(x) + \frac{df_1}{dx}dx$ і $f_2(x) + \frac{df_2}{dx}dx$.

На рис. 5 перша критична точка $x_{кр1}$ відсутня. Це характерно для систем, в яких один з об'єктів описується дробно-лінійною функцією $f(\tilde{x}) = \frac{\tilde{x}}{\tilde{x} + c}$. Відзначимо також, що подібна ситуація спостерігається у випадку двох однакових об'єктів: існує одна критична

точка $x_{кр}$, причому при $x < x_{кр}$ ресурси слід концентрувати на одному з об'єктів, а при $x > x_{кр}$ – поділяти порівну між об'єктами (рис. 7).

Аналізуючи положення характерних точок, можна зробити такі висновки:

1. Точка $x_{кр\,1}$ близька до точки перетину кривих $f_1(x_1)$, $f_2(x_2)$ (на рис. 3а, 3б $x_{кр\,1} = 0{,}069$ і $x_{кр\,1} = 0{,}049$, точка перетину кривих на рис. 1а, 1б $x = 0{,}070$ і, відповідно, $x = 0{,}051$).

2. Точка $x_{кр\,3}$ близька до точки перетину похідних $f_1'(x_1)$, $f_2'(x_2)$ (на рис. 3а, 3б $x_{кр\,3} = 0{,}179$ і $x_{кр\,3} = 0{,}111$, точки перетину похідних на рис. 1а, 1б $x = 0{,}180$ і, відповідно, $x = 0{,}111$).

3. Значення $x_{кр\,2}$ дещо перевищує $x_{кр\,3}$, а після стрибка x_2 стає близьким до нього (на рис. 3б $x_2 = 0{,}103$, а $x_{кр\,3} = 0{,}111$).

Приведені результати дозволяють оцінити кількість і розподіл ресурсів нападу, що буде корисним при розробці ефективних заходів протидії. Використовуючи описану методику і знайдені ресурси нападу, можемо визначити оптимальний розподіл ресурсів захисту. Продовжуючи цю процедуру, зрештою прийдемо до динамічного управління ресурсів в інформаційному протистоянні.

Література

1. Gordon L.A., Loeb M.P., The Economics of Information Security Investment, ACM Transactions on Information and System Security, Nov. 2002. – vol.5, №4. – P.438-457.

2. 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.

3. Левченко Є.Г., Оптимізація розподілу ресурсів між об'єктами захисту інформації. – К.: НТЖ «Захист інформації», – 2007, – №1. – С.34-38.

4. Левченко Є.Г., Рабчун А.О., Оптимізаційні задачі менеджменту інформаційної безпеки, НТЖ «Сучасний захист інформації», – 2010, – №1. – С.16-23.

Надійшла: 16.05.2011 р.

Рецензент: д.т.н., проф. Щербак Л.М.