УДК 004.681

ВПЛИВ ВРАЗЛИВОСТІ ОБ'ЄКТІВ НА РОЗВ'ЯЗОК ПРЯМОЇ ТА ЗВОРОТНОЇ ЗАДАЧ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

М.В. ДЕМЧИШИН, Є.Г. ЛЕВЧЕНКО

Оптимізація розподілу ресурсів між об'єктами захисту інформації ведеться на основі математичної моделі, в якій цільова функція визначає кількість вилученої інформації. Розглянуто та графічно проілюстровано ситуації, коли слід переходити від концентрації ресурсів на одному з об'єктів до їх розподілу між об'єктами. Показано, як впливає ймовірність виділення нападом певної кількості ресурсів на кінцевий результат.

ВСТУП

У математичних моделях менеджменту інформаційної безпеки цільова функція зазвичай визначає один із показників протистояння (часто — його оптимальне значення) через виражену в той чи інший спосіб вразливість системи захисту інформації (СЗІ) [1–4]. У моделі Гордона-Лоеба (ГЛ) [1–3] таким показником є зменшення втрат від вилучення інформації завдяки внесенню інвестицій із відрахуванням витрат y на її захист, а вразливість об'єкта розглядається як імовірність того, що напад буде успішним при $y = 0$.

ПОСТАНОВКА ЗАДАЧІ

У [4] цільова функція має вигляд:

$$I(x,y) = \sum_{k=1}^{l} I_k(x,y) = \sum_{k=1}^{l} G_k p_k q_k(x,y) f_k(x,y), \qquad (1)$$

де $l(x,y)$ — відносна кількість вилученої інформації; $k = \overline{1,l}$ — номер об'єкта захисту інформації; G_k — обсяг інформації на k-му об'єкті, $\sum_{k=1}^{l} G_k = G$; x та y — ресурси нападу і, відповідно, захисту, які віднесені до G_k; p_k — імовірність нападу на k-й об'єкт; $q_k(x,y)$ — імовірність виділення ресурсів x при нападі на k-й об'єкт; $f_k(x,y)$ — залежність частки вилученої інформації на k-му об'єкті від співвідношення x та y.

У [4] для різних інформаційних систем і умов протистояння наведено огляд актуальних задач, які можуть бути розглянуті за допомогою описаної методики.

Мета роботи — розв'язання однієї з таких задач, а саме — визначення оптимального розподілу ресурсів захисту по об'єктах, при якому досягаєть-

ся мінімум вилученої інформації. Частинні випадки цієї задачі розглянуто в [5], а формулювання задач для різних систем і умов протистояння — у [4].

МЕТОДИКА РОЗРАХУНКІВ ТА РЕЗУЛЬТАТИ

Під час застосування функції (1) ключовим питанням є встановлення явної форми залежностей $f_k(x, y)$ та їх фізичного змісту, тобто зв'язку з характеристиками об'єктів. Об'єкти можуть мати як фізичну природу (приміщення, паперова документація, канали витоку інформації), так і електронну (поштові сервери, файл-сервери тощо). Ці залежності мають задовольняти цілій низці вимог. Для того, щоб виокремити їх вплив, покладемо $p_k = 1$, $q_k(x, y) = \text{const} = 1$ і одержимо спрощену форму виразу (1):

$$I(x, y) = \sum_{k=1}^{l} G_k f_k(x, y). \qquad (2)$$

Таким чином, об'єкти на першому етапі нашого розгляду відрізняються лише двома показниками — обсягом інформації та залежністю $f_k(x, y)$, яку можна трактувати як характеристику вразливості об'єкта, яку визначимо як відношення кількості вилученої інформації до затрачених ресурсів: $\upsilon = \dfrac{I}{X}$. Надалі маленькими літерами позначатимемо відносні величини:

$$g_k = \frac{G_k}{G};\ i_k = \frac{I_k}{G};\ x_k = \frac{X_k}{G};\ y_k = \frac{Y_k}{G}.$$

Під час розгляду функціональних залежностей індекси опускаємо.

Основна вимога до залежностей $f(x, y)$: при $\dfrac{x}{y} \to 0$ $f(x, y) \to 0$, при $\dfrac{x}{y} \to \infty$ $f(x, y) \to a$, де $a \le 1$ — максимально можлива кількість вилученої інформації, яка визначається специфікою об'єкта та його системи захисту. Цим умовам відповідають степеневі $f(x, y) = \dfrac{a(x/y)^n}{(x/y)^n + c}$ і показникові $f(x, y) = a(1 - e^{-m(x/y)^n})$ функції [4]. Враховуючи, що за відповідного вибору параметрів ці залежності можуть стати досить близькими, обмежимось розглядом степеневих функцій. Параметри n та c у степеневій функції $f(x, y)$ можна встановити, виходячи з таких міркувань.

- При $x/y >> 1$ залежності $f(x, y)$ при різних n та c повинні мати схожий характер, який відповідає умові $f(x, y) \to a$. При $\sim x/y \gtrsim 0$ опуклість кривої може бути направлена як вгору, так і вниз — залежно від початкової вразливості об'єкта. У математичному виразі степеневої залежності $f(x, y)$ опуклість направлена вгору при $n \le 1$ та вниз — при $n > 1$.

- Вважаючи, що втрата 10–15 % інформації для підприємства є досить відчутною, а 15–20 % — критичною, формулюємо умову: при $x/y \approx 1$ — $i(x,y) \approx 0{,}05..0{,}15$, при $x/y \approx b$ — $i(x,y) \approx 0{,}2..0{,}3$. Граничне значення $x/y \approx b$ обирається з таких міркувань. Кількість ресурсів, які можуть бути виділені на захист інформації, за статистичними оцінками становить $y \approx 0..0{,}15g$. Вважаємо, що витрати ресурсів сторони нападу лежать в інтервалі $x \approx 0..0{,}5g$ (подальше їх збільшення визнаємо недоцільним). Виходячи з реальних граничних витрат та вважаючи, що витрати обох сторін визначаються одними і тими ж показниками (важливістю об'єкта та його вразливістю) і тому змінюються синхронно, отримуємо граничне значення $x/y = \dfrac{0{,}5}{0{,}15} \approx 3$. Надалі ресурси нападу подаватимемо у відносних величинах у двох варіантах: віднесені до кількості інформації — $x_k = \dfrac{X_k}{G_k}$, $x_k = 0..1$ або до ресурсів захисту — $x_k / y_k = 0..3$. Значення x/y, які лежать за межами цього інтервалу (зокрема, при $y \to 0$ $x/y \to \infty$) можуть бути розглянуті окремо. Варто зазначити, що наведені величини є орієнтовними і в окремих випадках можуть бути перевищені.
- При невеликих значеннях x/y ($x/y \lesssim 1$) СЗІ має бути рентабельною, тобто зменшення втрат інформації ΔI має перевищувати витрати y на її захист. При значних величинах $x/y \approx 3$ рентабельним має бути напад: $i \gtrsim x$.

Для того, щоб мати можливість графічно зображати результати, розглянемо систему з двох об'єктів. Оскільки цю роботу спрямовано на аналіз дій нападу з метою розробки заходів протидії, вважатимемо величини, які визначаються стороною захисту, сталими та рівними: $g_1 + g_2 = g = 1$, $y_1 + y_2 = y = 0{,}05g$ При прийнятих допущеннях щодо p_k та $q_k(x,y)$ маємо $i_k(x,y) = g_k f_k(x,y)$. Степеневі залежності $f(x,y)$, які відповідають визначеним вимогам і показують вплив параметрів *a*, *n* та *c* наведено на рис. 1.

Вважаючи, що об'єкти мають різний ступінь вразливості та враховуючи наведені вище умови, оберемо функції $f(x,y)$ для двох об'єктів у формі (рис. 1):

$$f_1(x,y) = \frac{1}{2}\frac{\dfrac{x_1}{y_1}}{\dfrac{x_1}{y_1}+3};\ f_2(x,y) = \frac{1}{3}\frac{\left(\dfrac{x_2}{y_2}\right)^3}{\left(\dfrac{x_2}{y_2}\right)^3+4}. \qquad (3)$$

Зазначимо, що коефіцієнти $\dfrac{1}{2}$ та $\dfrac{1}{3}$ введені у вирази $f_k(x,y)$ (3) для того, щоб підкреслити кривизну ліній, що, звичайно, не обмежує загальність дослідження.

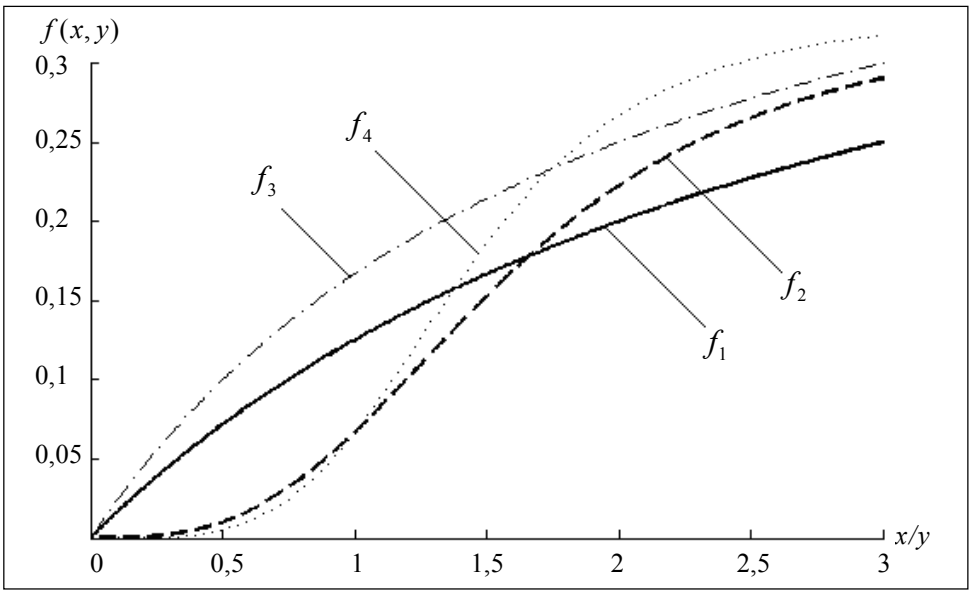

Рис. 1. Степеневі залежності $f(x, y)$ при різних значеннях параметрів

Опуклість у початковій області об'єкта 1, відповідно до (3), направлена вгору, що свідчить про низький рівень початкової вразливості, а для об'єкта 2 картина протилежна (рис. 1). Прикладом елементу захисту, для якого характерна форма залежності 2, є шифрування даних. Для зламу цієї системи потрібна значна кількість ресурсів, проте після досягнення цієї мети кількість вилученої інформації стрімко зростає.

Цільова функція (2) із врахуванням (3) приймає вигляд:

$$i(x_1, x_2, y_1, y_2) = i_1(x_1, y_1) + i_2(x_2, y_2) = \frac{1}{2} g_1 \frac{\frac{x_1}{y_1}}{\frac{x_1}{y_1} + 3} + \frac{1}{3} g_2 \frac{\left(\frac{x_2}{y_2}\right)^3}{\left(\frac{x_2}{y_2}\right)^3 + 4}. \quad (4)$$

Використовуючи (4), можна сформулювати оптимізаційні задачі двох типів:

- *пряма задача* — при заданій кількості ресурсів нападу $x_1 g_1 + x_2 g_2 = x$ знайти оптимальний розподіл $\{x_1^0, x_2^0\}$, який забезпечує максимальну кількість вилученої інформації $i_{\max}$ (надалі через x та y позначатимемо сумарні ресурси двох об'єктів);
- *зворотна задача* — знайти необхідну кількість ресурсів $x_1 g_1 + x_2 g_2 = x$ та їх розподіл, який забезпечує вилучення заданої кількості інформації i.

Графічну ілюстрацію розв'язку обох задач наведено на рис. 2. Значення X, Y, Z в інформаційних полях позначених точок зображають величини, які наведені на відповідних вісях координат — у цьому випадку x_1, x_2, $i(x, y)$.

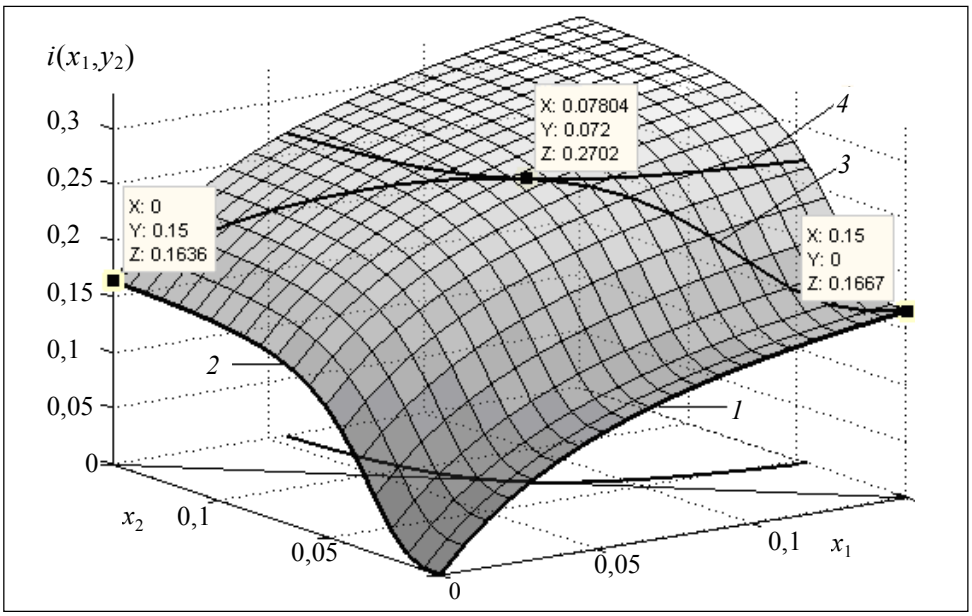

Рис. 2. Графічна ілюстрація розв'язку прямої та зворотної задач

Розглянемо спочатку розв'язок *прямої задачі*. Задаємо кількість ресурсів нападу (для прикладу візьмемо $x = 0{,}15$) і будуємо обмежувальну пряму $x_1 + x_2 = 0{,}15,$ а потім здійснюємо переріз об'ємної фігури $i(x_1, x_2)$, побудованої на залежностях $i_1(x_1),\ \ i_2(x_2)$ при $g_1 = g_2 = 0{,}5,\ \ y_1 = y_2 = 0{,}025,$ $y_1 + y_2 = 0{,}05,\ \ y_1 g_1 + y_2 g_2 = 0{,}025$ (криві 1 та 2) вертикальною площиною, що проходить через цю пряму (у виразі $i_k(x, y)$ величину $y = \text{const}$ опускаємо). Лінія 3, утворена цим перерізом, визначає множину всіх можливих значень $i(x_1, x_2)$ і дає змогу знайти $i_{\max}$ та відповідний розподіл x_1^0, x_2^0 (на рис. 2 $x_1^0 = 0{,}078$, $x_2^0 = 0{,}072$, $i_{\max} = 0{,}27$).

Кількість максимумів, які має функція $i(x_1, x_2)$ при обмеженні $x_1 + x_2 = x$ визначається формою складових $i_1(x_1),\ \ i_2(x_2)$. Один максимум спостерігається у випадку, коли кожна зі складових виражається однією дробно-лінійною або дробно-нелінійною функцією, тобто похідні $i_1'(x_1),$ $i_2'(x_2)$ мають не більше одного максимуму. У протилежному випадку можна спостерігати декілька локальних максимумів. Максимальне значення функція може приймати і на кінці інтервалу, що відображає ситуацію, коли всі ресурси слід вкладати в один із об'єктів.

Як видно з (4), на величини $i(x_1, x_2)$ і, відповідно, $i_{\max}$, крім виду залежностей $f_1(x, y)$ та $f_2(x, y),$ має вплив також розподіл g_1/g_2 інформації між об'єктами. При зміні цього співвідношення криві $i_1(x_1),$ та $i_2(x_2)$ на рис. 2 будуть змінювати своє положення: одні підніматись, а інші — опускатись. При цьому буде змінюватись форма просторової фігури $i(x_1, x_2)$, форма ліній перерізу і значення оптимальних величин.

Розглянемо тепер *зворотну задачу*. Її розв'язок одержимо в результаті перерізу поверхні $i(x_1, x_2)$ площиною $x_1 0 x_2$, проведеною на рівні

$i(x_1, x_2) = C$ (рис. 2). Точка дотику отриманої в результаті перерізу лінії рівня (ізокванти) $i(x_1, x_2) = C$ (крива 4) і обмежувальної прямої (ізокости) $x_1 + x_2 = x$ дає розв'язок задачі, тобто значення x, яке забезпечує вилучення інформації $i(x_1, x_2) = C$ і відповідний оптимальний розподіл $\{x_1^0, x_2^0\}$, а саме, розподіл, який забезпечує задану величину $i(x_1, x_2)$ при мінімальному значенні $x_1 + x_2 = x$. На рис. 2 переріз здійснено на рівні $C = i_{\max} = 0{,}27$, визначеному розв'язком прямої задачі. На рис. 3 показано положення ліній перерізу і точок дотику до обмежувальних прямих $x_1 + x_2 = x$, які визначають оптимальні величини x_1^0, x_2^0 для різних значень $i(x_1, x_2)$: *1* — $i = 0{,}3$, *2* — $i = 0{,}27$, *3* — $i = 0{,}2$, *4* — $i = 0{,}1$.

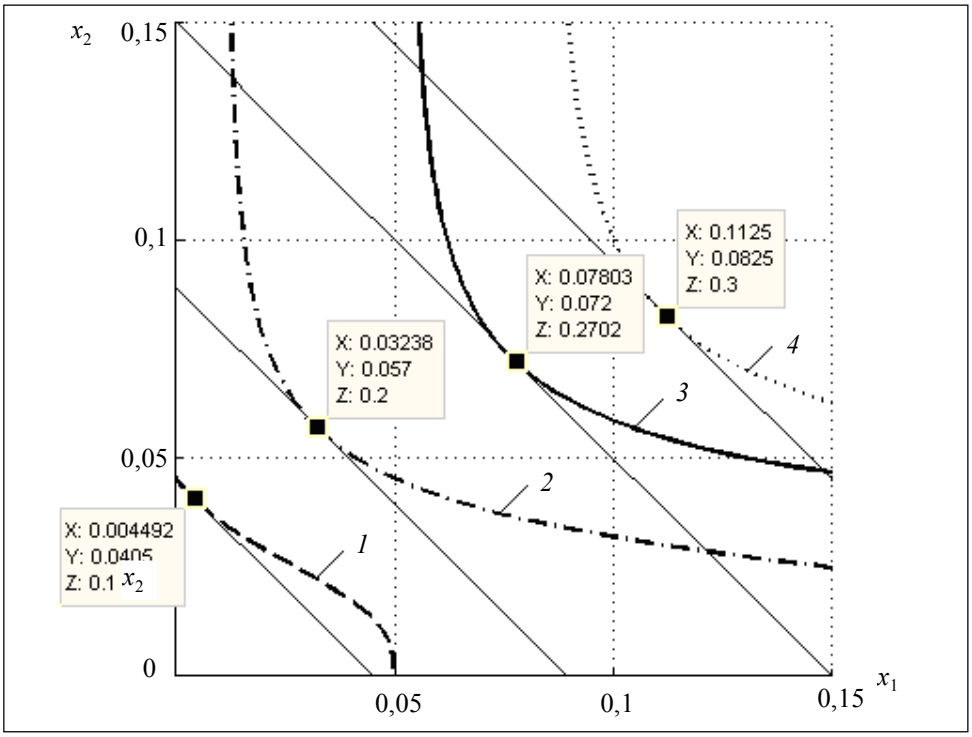

Рис. 3. Формування оптимального розподілу ресурсів нападу

Необхідні значення ресурсів нападу x для деяких значень i, а також оптимальні розподіли $\{x_1^0, x_2^0\}$ для них, розраховані за виразом (4) при $g_1 = g_2 = 0{,}5$, $y_1 = y_2 = 0{,}025$, наведено в таблиці.

Таблиця. Величини x та оптимальні розподіли $\{x_1^0, x_2^0\}$ ресурсів нападу, які необхідні для вилучення заданої кількості інформації $i(x_1, x_2)$

$i(x_1, x_2)$	**0,1**	**0,2**	**0,27**	**0,3**
x	0,045	0,089	0,15	0,195
x_1^0	0,005	0,032	0,078	0,112
x_2^0	0,04	0,057	0,072	0,082

Результати, наведені в третьому стовпчику таблиці, є розв'язком зворотної задачі, де вхідні дані взято з попередньо знайденого розв'язку прямої задачі ($i(x_1, x_2) = 0{,}27$ для $x = 0{,}15$). В інших стовпчиках мають місце розв'язки зворотної задачі для довільних значень $i(x_1, x_2)$.

Таким чином, обмежувальна пряма $x_1 + x_2 = x$ своїм дотиком до ліній, утворених перерізом поверхні $i(x_1, x_2)$ двома взаємно перпендикулярними площинами, визначає точку оптимізації, яка, у свою чергу, після проектування на площину $x_1 0 x_2$, задає оптимальний розподіл (x_1^0, x_2^0). Кількісні результати, наведені в таблиці, розраховані з використанням функції fmincon пакету Optimization Toolbox програмного комплексу Matlab. Ця функція знаходить мінімум скалярної функції багатьох змінних при обмеженнях типу $Ax \le B$. Графічна інтерпретація надається лише для ілюстрації сутності явища.

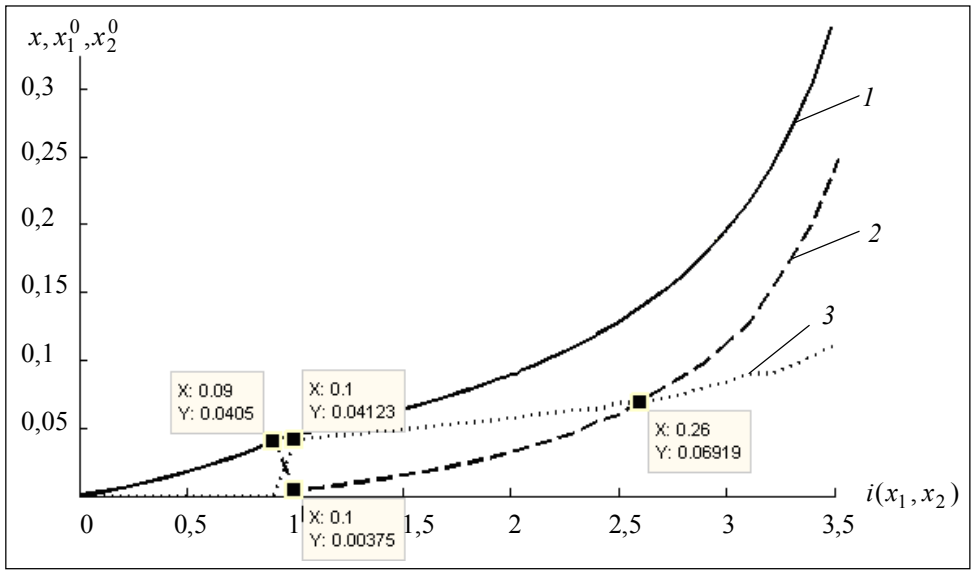

Рис. 4. Розподіл ресурсів при розв'язку зворотної задачі, крива *1* — x, *2* — x_1^0, *3* — x_2^0

На рис. 4 наведено залежність x від величини i, а також оптимальні розподіли x_1^0, x_2^0 для різних i. Інтервал можливих значень i обрано з огляду на розрахункові значення $f(x, y)$ з рис. 1. Цікавим на цьому графіку є наявність двох критичних точок $i_{\text{кр}}^{(1)}$ та $i_{\text{кр}}^{(2)}$. При $i < i_{\text{кр}}^{(1)}$ всі ресурси нападу доцільно зосередити на одному з об'єктів. Цей об'єкт визначається кількістю інформації на ньому і ступенем його вразливості. На рис. 4 $i_{\text{кр}}^{(1)} = 0{,}09$, при $i < 0{,}09$ $x_1^0 = x$, $x_2^0 = 0$. При $i > i_{\text{кр}}^{(1)}$ відбувається перерозподіл ресурсів нападу: x_1^0 суттєво зменшується (з 0,0405 до 0,00375), а x_2^0 стрибком зростає від 0 до 0,04123. При подальшому збільшенні x обидві величини x_1^0 та x_2^0 зростають, причому $x_2^0 > x_1^0$. При $i = i_{\text{кр}}^{(2)}$ вони досягають

однакового значення ($x_1^0 = x_2^0 = 0{,}06919$), після чого x_1^0 перевищує x_2^0. Використовуючи економічну термінологію, можемо вважати, що $i_1(x)$ та $i_2(x)$ — субститути, а перехід від одного об'єкта до іншого характеризує еластичність доходу.

Наявність критичних точок можна пояснити такими причинами. На початковому етапі зростання x $i_1(x) > i_2(x)$ та $i_1'(x) > i_2'(x)$, тобто кількість інформації, яка вилучається з першого об'єкта, і швидкість зростання цієї кількості перевищують відповідні величини для другого об'єкта (криві 1 та 2 на рис. 1). При такому припущенні про однакову кількість інформації на об'єктах ($g_1 = g_2$) це може бути спричинено більшою початковою вразливістю першого об'єкта. У цих умовах доцільно направляти всі ресурси нападу на перший об'єкт: $x_1^0 = x$. Проте зі збільшенням x значення $i_1'(x)$ зменшується, а значення $i_2(x)$ та $i_2'(x)$ зростають, що зрештою призводить до ситуації, коли сума $g_2 i_2(x_2) + g_1 i_1(x - x_2)$ стає більшою, ніж $g_1 i_1(x_1)$. У цій точці доцільно перейти до розподілу ресурсів між двома об'єктами. Значення $i_{\text{кр}}^{(1)}$ визначається кривизною ліній $f_1(x)$, $f_2(x)$ та співвідношенням g_1/g_2. Під час переходу через цю точку залежність $x(i)$ змінює свій нахил, оскільки до цієї точки вона повністю визначається функцією $i_1(x)$, а при $i > i_{\text{кр}}^{(1)}$ — обома функціями $i_1(x)$, $i_2(x)$. Зменшення нахилу $i(x)$ свідчить про перехід до ефективнішого використання ресурсів нападу.

Отриманий результат деякою мірою перегукується з висновками [1], де ставиться задача оптимізації загальної кількості виділених ресурсів захисту і при деяких видах залежності кількості вилученої інформації i від вразливості υ оптимальна кількість ресурсів захисту $y = y^0$ дорівнює нулю при малих, а в деяких випадках — також при дуже великих значеннях вразливості.

Стрибкоподібний перерозподіл ресурсів у точці $i_{\text{кр}}^{(1)}$ можна проілюструвати ще за допомогою геометричної інтерпретації розв'язку (рис. 5), де показано, що в інтервалі $x \le 0{,}04358$ ресурси нападу доцільно направляти на перший об'єкт, а при перевищенні цього значення розподіляти між об'єктами (квадратики — точки, в яких $x \to \min$).

Значення x_1^0, x_2^0 у рисунках обираються такими, щоб сума ординат на кривих 1, 2 рис. 1 під час виконання обмежувальної умови набувала максимального значення. Це фактично є формулюванням принципу Лагранжа, який у застосуванні до нашої задачі дає змогу одержати аналітичні вирази для x_1^0, x_2^0.

Запишемо функцію Лагранжа, подаючи лінійну та кубічну залежності $f_k(x, y)$ в загальній формі:

$$L(x_1, x_2, \lambda) = g_1 \frac{a_1(x_1/y_1)}{x_1/y_1 + c_1} + g_2 \frac{a_2(x_2/y_2)^3}{(x_2/y_2)^3 + c_2} - \lambda(x_1 + x_2 - x).$$

Беручи частинні похідні по невідомим x_1, x_2, λ, одержуємо систему рівнянь, яка визначає x_1^0, x_2^0, λ:

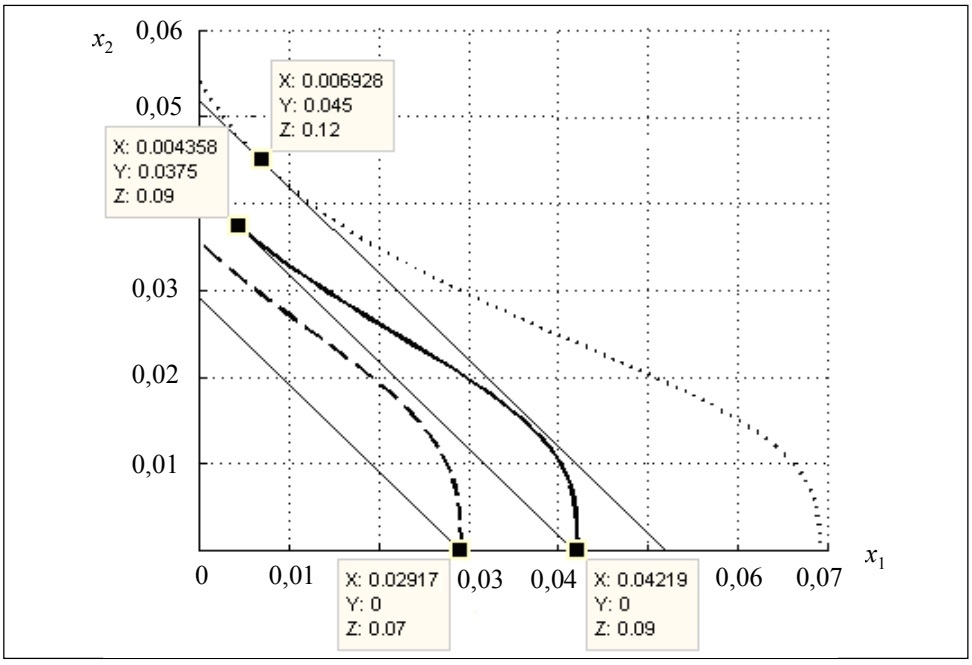

Рис. 5. Графічне пояснення стрибкоподібного перерозподілу ресурсів

$$\begin{cases} x_1^0 = \sqrt{\dfrac{a_1 c_1}{\lambda} g_1 y_1} - c_1 y_1 \\ \left(x_2^0 / y_2\right)^3 - \sqrt{\dfrac{3 g_2 a_2 c_2}{\lambda}} \left(x_2^0 / y_2\right) + c_2 = 0. \\ x_1^0 + x_2^0 = x \end{cases}$$

Розв'язок значно спрощується, якщо обидві залежності $f_1(x,y)$, $f_2(x,y)$ виражаються функціями першого степеня:

$$f_1(x,y) = \frac{a_1 (x_1/y_1)}{x_1/y_1 + c_1};\ f_2(x,y) = \frac{a_2 (x_2/y_2)}{x_2/y_2 + c_2}.$$

Тоді шукані величини можна записати в явній формі:

$$x_1^0 = \sqrt{\frac{a_1 c_1}{\lambda} g_1 y_1} - c_1 y_1;\ \ x_2^0 = \sqrt{\frac{a_2 c_2}{\lambda} g_2 y_2} - c_2 y_2;$$

$$\lambda = \frac{\left(\sqrt{a_1 c_1 g_1 y_1} + \sqrt{a_2 c_2 g_2 y_2}\right)^2}{\left(x + c_1 y_1 + c_2 y_2\right)^2}.$$

Врахуємо тепер *залежність* $q(x,y)$, в якій y задається як параметр. Вид цієї залежності можна встановити з таких міркувань. Зрозуміло, що

$q(x,y) \to 0$ при $x \to 0$ та при $x \to \infty$, отже $q(x,y) \to \max$ при певному значенні x (оскільки $q(x,y) \geq 0$). Вважатимемо, що ймовірність виділення ресурсів пропорційна обсягу інформації на об'єкті та його вразливості, яку визначаємо як $\upsilon_k = \dfrac{i_k}{x_k} = \operatorname{tg}\alpha_k$, де α_k — кут між віссю абсцис і прямою, проведеною з початку координат у точку на кривій (рис. 1), яка відповідає певному значенню $f_k(x,y) = i_k(x,y)$. Розраховані таким чином величини $\upsilon_k(x,y)$, що відповідають залежностям $f_1(x,y)$, $f_2(x,y)$ (3), зображено на рис. 6 (криві 1, 2).

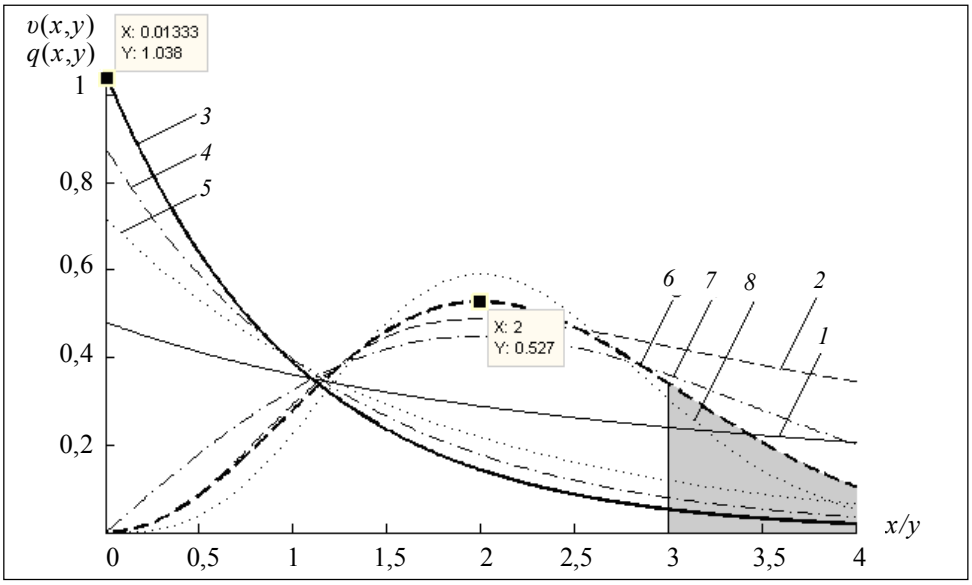

Рис. 6. Формування залежності $q(x,y)$ в обмеженому інтервалі значень x/y

Зазначимо, що використати залежність $\upsilon(x,y)$ у «чистому» вигляді в якості $q(x,y)$ неможливо. Це пояснюється тим, що при зростанні x вразливість $\upsilon = \operatorname{tg}\alpha_k$, виражена залежностями $f(x,y)$ (рис. 1), спадає досить повільно (рис. 6, криві 1, 2), тоді як імовірність нападу при $x \gtrsim g$ прямує до нуля (через нерентабельність). Тому під час формування залежності $q(x,y)$ слід, крім вразливості, врахувати ще й доцільність нападу, яка визначається рентабельністю вкладених ресурсів $r = \dfrac{i-x}{x} = \upsilon - 1$. Слід зазначити, що введене поняття вразливості відрізняється від вразливості [1], яка визначається як імовірність успішного здійснення нападу і не пов'язана явно з кількістю вилученої інформації. Вразливість у нашій інтерпретації пов'язана з рентабельністю і за позитивного її значення $\upsilon > 1$. Інтервал можливих значень x у виразі $q(x,y)$ обмежений певним значенням $x_{\text{гр}}$, яке визначається умовою:

$$\int_0^{x_{\text{гр}}} q(x,y)dx = 1. \qquad (5)$$

Звуження інтервалу x викликає необхідність деформування залежності $q(x,y)$ порівняно з $\upsilon(x,y)$: у межах $0..x_{\text{гр}}$ її слід підняти, а за межами цього інтервалу — опустити, відкинувши «хвіст» розподілу з точки $x_{гр}$. Ступінь деформації в інтервалі $0..x_{\text{гр}}$ визначається умовою (5). Точка $x = x_m$, за якої досягається максимум $q(x,y) = q_m$, при деформації залишається незмінною, оскільки відповідає максимальному значенню вразливості.

Враховуючи, що вразливості об'єктів істотно різняться, оберемо для кожного з них свою залежність $q(x,y)$ (рис. 6). Для першого об'єкта форму залежності $\upsilon(x,y)$ подамо у вигляді функції

$$q_{11}(x,y) = Ne^{-\alpha\frac{x}{y}} = 1{,}05e^{-\frac{x}{y}}. \qquad (6)$$

Форма кривої $\upsilon(x,y)$ для другого об'єкта показує, що залежність $q(x,y)$ можна обрати у вигляді розподілу Максвела:

$$q_{21}(x,y) = N\left(\frac{x}{y}\right)^2 e^{-h^2\left(\frac{x}{y}\right)^2} = 0{,}36\left(\frac{x}{y}\right)^2 e^{-0{,}25\left(\frac{x}{y}\right)^2}, \qquad (7)$$

де $h = \dfrac{1}{x_m}$. Перший індекс в (6), (7) — номер об'єкта, другий — номер варіанта. Розрахунок нормовочних коефіцієнтів N в (6), (7) знаходимо з умови (5). Сталу h у цьому випадку визначаємо, поклавши $x_m = 2$. Значення $x_{\text{гр}}$ випливає з прийнятого інтервалу обмеження $x = 0..0{,}15$ і становить $x_{\text{гр}} = 0{,}15$, що, при обраному значенні $y = 0{,}05$, відповідає відношенню $x/y = 3$. Ступінь відхилення прийнятого розподілу $q(x,y)$ (крива 6 в межах $x/y = 0..3$) від розподілу Максвела визначається відносною площею відкинутого «хвоста» — $\Delta S = 0{,}21$ (заштрихована область).

Для порівняння на рис. 6 показано також інші залежності, які можна використовувати для апроксимації функцій $q(x,y)$ Для першого об'єкта (криві 4, 5):

$$q_{12}(x,y) = 0{,}88e^{-0{,}8\frac{x}{y}},\ q_{13}(x,y) = 0{,}719e^{-0{,}6\frac{x}{y}}. \qquad (8)$$

Для другого об'єкта — розподіл Релея (крива 7) та кубічна залежність (крива 8):

$$q_{22}(x,y) = 0{,}37\left(\frac{x}{y}\right)e^{-0{,}125\left(\frac{x}{y}\right)^2},\ q_{23}(x,y) = 0{,}331\left(\frac{x}{y}\right)^3 e^{-0{,}375\left(\frac{x}{y}\right)^2}. \qquad (9)$$

Вибір функції $q(x,y)$ для кожного об'єкта визначається його динамічною вразливістю, яка випливає із залежностей $f(x,y)$ (рис. 1).

На рис. 7 зображено залежності $i_{kn} = g_k f_{kn}$, які розраховані на основі (1) за умови, що $g_k = 0{,}5$, $p_k = 1$, $y_k = 0{,}025$, $f_k(x, y)$ задається виразами (3), $q_{kn}(x, y)$ — виразами (6)–(9).

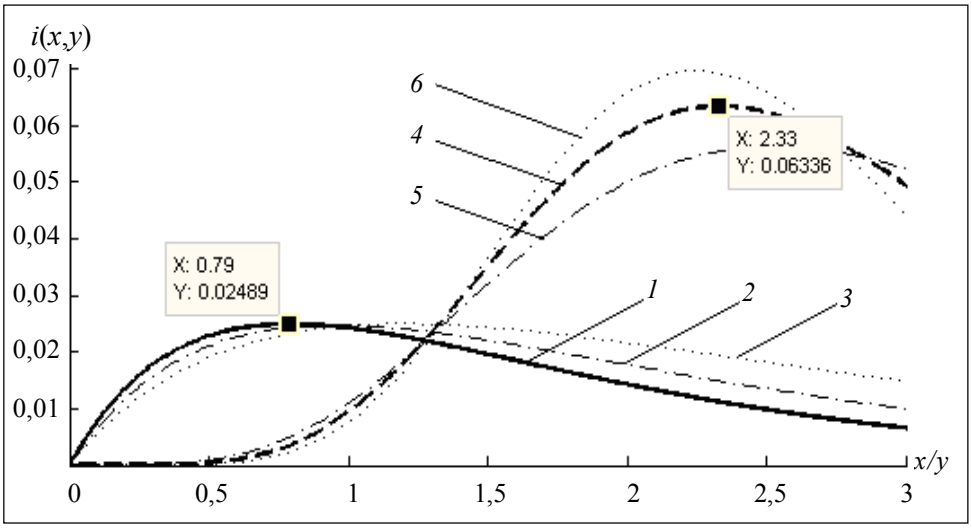

Рис. 7. Функції $i(x, y)$ з врахуванням залежностей $q(x, y)$

Із врахуванням залежностей $f_k(x, y)$, $q_{kn}(x, y)$, які відповідають виразам (3), (6), (7), цільова функція $i(x_1, x_2)$, що визначає відносну кількість вилученої інформації з двох об'єктів, має вигляд:

$$i(x, y) = g_1 q_{11}(x_1, y_1) f_1(x_1, y_1) + g_2 q_{21}(x_2, y_2) f_2(x_2, y_2) =$$

$$= \frac{1}{2} g_1 1{,}05 e^{-\frac{x_1}{y_1}} \frac{\frac{x_1}{y_1}}{\frac{x_1}{y_1} + 3} + \frac{1}{3} g_2 0{,}36 \left(\frac{x_2}{y_2}\right)^2 e^{-0{,}25\left(\frac{x_2}{y_2}\right)^2} \frac{\left(\frac{x_2}{y_2}\right)^3}{\left(\frac{x_2}{y_2}\right)^3 + 4}. \quad (10)$$

Графічне зображення об'ємної фігури, яка відповідає цій функції, наведено на рис. 8. Використання залежності $q(x, y)$ викликає деформацію фігури рис. 2. У результаті з'являється вершина «гори» (рис. 8), яка визначає абсолютний максимум $i_{\max} = 0{,}06498$ і оптимальний розподіл ресурсів $x_1^0 = 0{,}0225$ та $x_2^0 = 0{,}105$, а також його сумарне значення $x^0 = 0{,}123$ при $g_1 = g_2 = 0{,}5$, $y_1 = y_2 = 0{,}025$.

Лінії рівня, отримані в результаті перерізу об'ємної фігури рис. 8 площинами $i(x_1, x_2) = C$ при різних C дозволяють скласти чіткіше уявлення про крутизну цієї фігури в різних напрямках (криві *1–3* на рис. 9). Для порівняння на цьому ж рисунку наведено лінії перерізу (криві *4–6*) ще однієї залежності $i(x_1, x_2) = g_1 q_{13}(x_1) f_1(x_1) + g_2 q_{23}(x_2) f_2(x_2)$. Перерізи здійснено на рівнях: криві *1*, *4* — $i(x_1, x_2) = 0{,}06$; *2*, *5* — $i(x_1, x_2) = 0{,}05$; *3*, *6* — $i(x_1, x_2) = 0{,}04$.

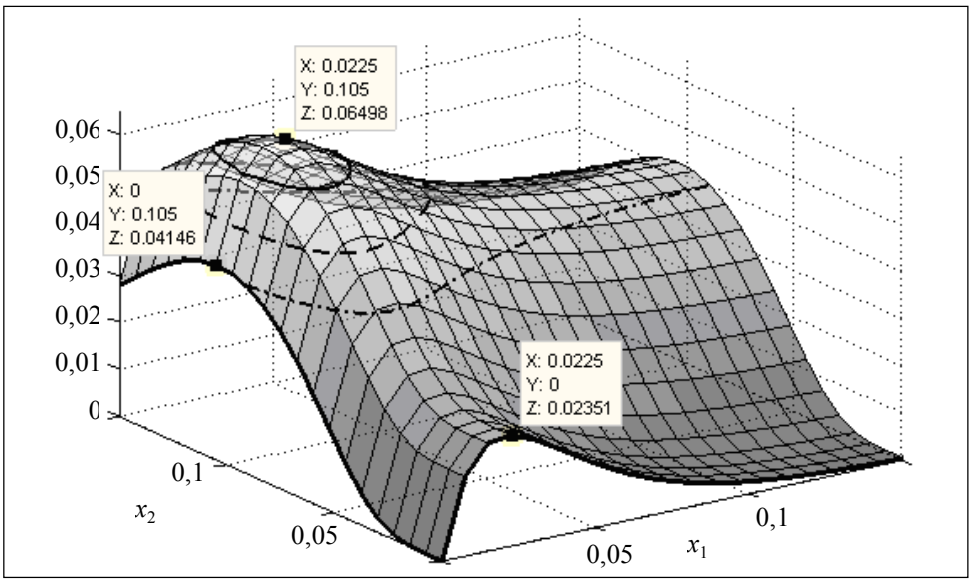

Рис. 8. Просторова фігура $i(x, y)$ із врахуванням залежностей $q(x, y)$

Густина ліній в околі точки $i_{\max}$ у горизонтальному та вертикальному напрямках дозволяє оцінити чутливість величини i до відхилення x_1 та x_2 від їх оптимальних значень x_1^0, x_2^0.

Підсумовуючи, нагадаємо, що кінцевою метою дослідження є пошук оптимальної стратегії дій захисту, тобто визначення оптимальних значень y_k^0. Розрахунок максимальних значень $i(x, y)$ та $\{x_k^0\}$ допомагає передбачити дії суперника та розробити заходи протидії.

Визначення оптимального відношення $(y_1/y_2)^0$ для системи з двох об'єктів проводиться в такій послідовності.

- На основі експертних оцінок визначаємо розподіл $\{g_k\}$.
- У результаті аналізу фізичної вразливості кожного об'єкта підбираємо залежності $f_1(x, y)$, $f_2(x, y)$.
- Поклавши $p_1 = p_2 = p = 1$ та вибравши вид функції $q(x, y)$, формуємо цільову функцію:

$$i(x, y) = g_1 q_1(x, y) f_1(x, y) + g_2 q_2(x, y) f_2(x, y).$$

- Виходячи з реальних можливостей, встановлюємо межі допустимих значень *x* та *y*, наприклад

$$y = (0..0{,}05)\, g\,, \quad x = (0..3) y = (0..0{,}15) g\,.$$

- Виходячи з умови досягнення максимальної рентабельності ресурсів нападу на кожному об'єкті, тобто враховуючи вираз для динамічної вразливості об'єкта, яка випливає з обраної залежності $f_k(x, y)$, визначаємо x_k/y_k.

• Враховуючи співвідношення g_1/g_2, υ_1/υ_2, задаємо $y_1/y_2 = g_1/g_2\,\upsilon_1/\upsilon_2$ і, знаючи $y = y_1 + y_2$, знаходимо y_1 та y_2.

• Задаємо g_1, g_2, y_1, y_2 у вираз (8) і, використовуючи функції пакета Optimization Toolbox програмного комплексу Matlab, знаходимо оптимальні значення $\{x_1^0, x_2^0\}$, які визначаються критерієм $i(x_1^0, x_2^0) = \min\limits_{x_1, x_2} i(x_1, x_2)$.

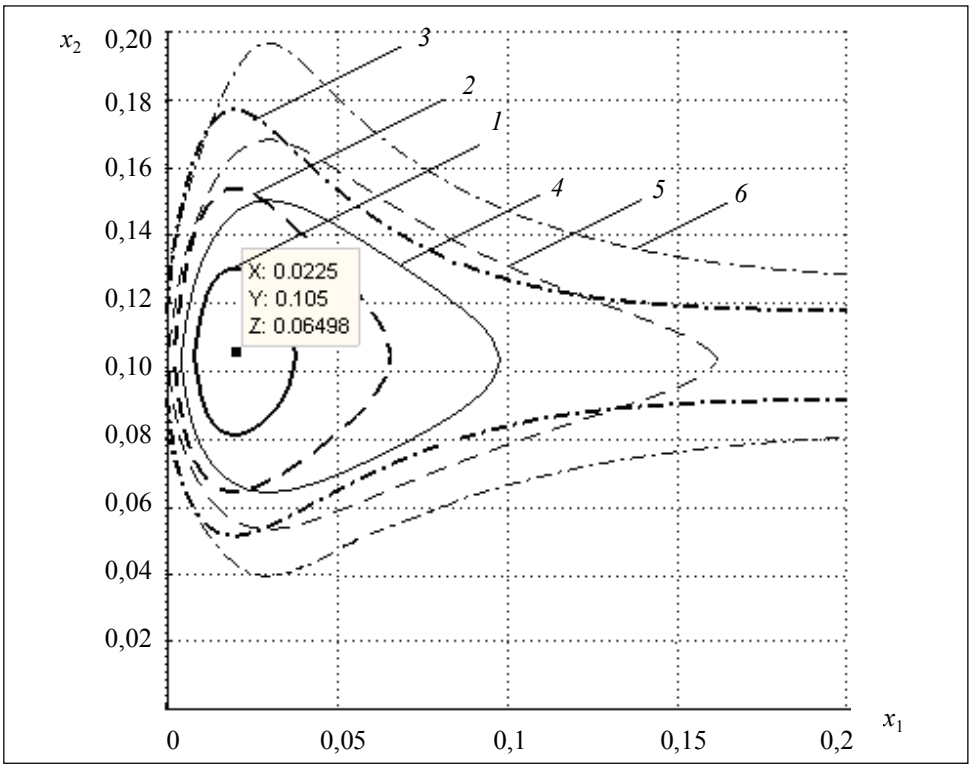

Рис. 9. Лінії рівня просторової фігури рис. 8

• Використовуючи значення $\{x_k^0\}$, повторюємо описану процедуру по відношенню до $\{y_k\}$ і знаходимо $\{y_k^0\}$, виходячи з критерію $i(y_1^0, y_2^0) = \min\limits_{y_1, y_2} i(y_1, y_2)$

ВИСНОВКИ

Зроблені у нашому розгляді обмеження та припущення не є принциповими і не звужують область застосування наведеної методики. Розроблену модель можна застосовувати до системи з довільною кількістю об'єктів при різних розподілах обсягів інформації та різній вразливості об'єктів.

Її обґрунтуванням може бути те, що вона дає якісно схожі, а при певному виборі параметрів — повністю співпадаючі результати з найбільш відомою і широко вживаною моделлю ГЛ, яка знайшла своє емпіричне підтвердження [6].

Окреслимо можливі напрями розвитку методики.

- Встановлення зв'язку між залежностями $f_k(x, y)$ і характеристиками об'єктів — як фізичних, так і електронних. На цій основі проводиться уточнення залежностей $f_k(x, y)$, $q_k(x, y)$.
- Розробка методики розв'язку багатопоказникової екстремальної задачі з використанням цільової функції, в яку входять декілька показників (наприклад, кількість вилученої інформації i та кількість ресурсів захисту y з певними ваговими коефіцієнтами).
- Розробка універсальної програми динамічного управління ресурсами в багаторубіжних системах в умовах комплексного протистояння, коли частина ресурсів кожної сторони витрачається на захист власної інформації, а інша частина — на здобуття інформації суперника з врахуванням можливості попереднього проведення розвідки.

ЛІТЕРАТУРА

1. *Gordon L.A., Loeb M.P.* The economics of information security investment // ACM Transactions on information and system security, Nov. — 2002. — **5**, № 4. — P. 438–457.
2. *Matsuura K.* Productivity space of information security in an extension of the Gordon-Loeb's investment model // The 7-th workshop on the economics of information security, Hanover, USA, June 25–28. — 2008. — http://weis2008.econinfosec.org/papers/Matsuura.pdf.
3. *Huang C.D., Hu Q., Behara R.S.* Economics of information security investment in the case of simultaneous attacks // Proceeding of the 5-th workshop on the economics of information security, Cambridge, England, June 26–28. — 2006. — P. 1–33.
4. *Левченко Є.Г., Рабчун А.О.* Оптимізаційні задачі менеджменту інформаційної безпеки // НТЖ «Сучасний захист інформації». — 2010. — № 1. — С. 16–23.
5. *Левченко Є.Г.* Оптимізація розподілу ресурсів між об'єктами захисту інформації. — К.: НТЖ «Захист інформації». — 2007. — № 1. — С. 34–38.

Надійшла 14.10.2010