УДК 004.056

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 2, pp. 167-176

ПОШУК ОПТИМАЛЬНОГО РІШЕННЯ ЗВОРОТНОЇ ЗАДАЧІ ЕКОНОМІЧНОГО МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Є.Г. Левченко, Д.І. Рабчун

Національний авіаційній університет,
просп. Космонавта Комарова, 1, Київ, 03058, Україна; e-mail: professor_va@ukr.net

Першим кроком до синтезу систем захисту інформації є рішення зворотної задачі, коли по заданим показникам системи знаходять необхідну кількість ресурсів і їх розподіл між об'єктами. Розглянуто інформаційну систему, котра містить два об'єкти і може функціонувати в двох режимах протистояння: однонаправленому, коли кожна сторона захищає свою інформацію, і двонаправленому, коли кожна з сторін захищає свою інформацію і прагне здобути інформацію суперника. Рішення зворотної задачі через її складність зводять до розв'язку прямої і шляхом перебору, використовуючи метод Белмана, знаходять необхідні величини. Враховуючи невизначеність умов протистояння в інформаційній сфері, необхідно знайти таке рішення, котре забезпечує задані показники при будь-яких діях суперника. В економічній теорії така ситуація відома як рівновага за Нешем. При геометричній інтерпретації результатів вона зображується сідловою точкою на просторовій фігурі, котра представляє цільову функцію в залежності від ресурсів обох сторін. Знайдено розв'язок зворотної задачі в інтервалах існування сідлової точки при різних значеннях параметрів системи. Встановлено вимоги до параметрів, виконання яких дозволяє одержати оптимальний результат.

Ключові слова: інформаційна безпека, математична модель, розподіл ресурсів, сідлова точка.

Вступ

Розвиток інформаційної сфери відображається в багатьох показниках: зростають обсяги і вартість інформації, частота і витонченість нападів, вартість втрат від витоку інформації та, відповідно, складність та вартість захисних структур. Як наслідок — зростають вимоги до ефективності використання ресурсів захисту, котра визначає, зрештою, технічні та економічні показники систем захисту інформації. Оптимізація кількості та розподілу ресурсів захисту являє собою досить серйозну задачу, труднощі рішення котрої пояснюються низкою причин: складність систем захисту, невизначеність умов протистояння, неможливість точного визначення параметрів і функціональних залежностей, котрі характеризують вразливість об'єктів захисту. Невизначеність умов протистояння в економічній сфері полягає в тому, що невідомі наміри, а іноді і дії суперника – націленість атак, кількість його ресурсів і їх розподіл між об'єктами. Розгляд всіх можливих ситуацій при пошуку оптимальної стратегії дії захисту приводить до значного зростання кількості розрахункових варіантів і, зрештою, не дає відповіді на поставлене питання. Часто ці труднощі обходять, оцінюючи імовірності окремих стратегій нападу і переходячи до пошуку рішення в умовах ризику [1]. Суб'єктивізм такого підходу в значній мірі знецінює отримані результати. Бажано знайти таке рішення, котре забезпечує певний результат за будь-яких дій суперника, що особливо важливо в умовах динамічного протистояння, коли умови протистояння

змінюються з часом. При графічному поданні результатів ця ситуація відображається сідловою точкою на просторовій фігурі, що зображає цільову функцію в залежності від ресурсів нападу і захисту [2].

Поряд з розв'язком прямої задачі, в якій по заданим ресурсам сторін знаходять показники протистояння, важливе прикладне значення має рішення зворотної задачі, коли по заданим показникам потрібно знайти необхідну кількість ресурсів і їх розподіл між об'єктами. Рішення цієї задачі відкриває шлях до синтезу систем захисту, котрий дозволяє визначити необхідні засоби для кожного з об'єктів.

Мета роботи – визначення кількості ресурсів захисту і їх розподілу між об'єктами, необхідних для досягнення заданих показників в умовах динамічного інформаційного протистояння.

Методика розрахунків і результати

При побудові системи захисту інформації необхідно врахувати природу об'єктів (фізичну чи електронну), їх кількість, параметри і характеристики, зокрема, початкову і динамічну вразливість, розподіл інформації по об'єктах, ймовірність нападу, кількість ресурсів, направлених на кожний з об'єктів, а також умови протистояння (однонаправлене чи різнонаправлене) і режим протистояння (статичний чи динамічний). В залежності від цих даних формується структура системи захисту – однорівнева чи багаторівнева, з послідовним, паралельним чи послідовно-паралельним розташуванням засобів захисту, а також типи цих засобів з врахуванням обмеження на їх загальну вартість, знайдену в результаті рішення оптимізаційної задачі.

При постановці оптимізаційної задачі першим кроком є визначення величини, яка підлягає оптимізації, а також форми цільової функції і критерію оптимальності. При розв'язку прямої задачі метою пошуку можуть бути:

1. Мінімум втрат інформації або сумарних втрат, котрі об'єднують втрати інформації і витрати на її захист;
2. Максимум прибутку від інвестиції в захист інформації або їх рентабельності.

Можливий також багатокритеріальний підхід, при якому цільова функція містить наведені величини з певними ваговими коефіцієнтами.

При розв'язку зворотної задачі задають граничні значення одного або декількох зазначених показників і визначають необхідну кількість ресурсів захисту і їх оптимальний розподіл між об'єктами. Критерієм оптимальності є досягнення кращих значень інших показників або їх комбінації. Прикладом такого підходу є задання гранично допустимого значення втрат інформації і визначення необхідної кількості ресурсів захисту та одночасно розподілу цих ресурсів між об'єктами, котрий відповідає мінімуму загальних втрат.

Слід зазначити, що рішення зворотної задачі через її складність часто зводять до прямої задачі і шляхом перебору одержаних розв'язків знаходять необхідний варіант. Оскільки виконання поставлених в умові обмежень необхідно забезпечити при будь-яких діях суперника, то бажано, щоб розв'язок знаходився в сідловій точці.

При всіх підходах до розв'язку прямої задачі базовою величиною, котра входить в усі варіанти цільової функції, є кількість втрат від витоку інформації. Виходячи з важливості цього показника формуємо цільову функцію як частку $i(x, y)$ втраченої інформації в системі і подамо її у вигляді [3]:

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

де x та y — вартість ресурсів нападу і, відповідно, захисту, $\sum_{k=1}^{l} x_k = X$; $\sum_{k=1}^{l} y_k = Y$;

$k = \overline{1,l}$ – номер об'єкта;

g_k – частка загального обсягу інформації, що містить *k*-й об'єкт, $\sum_{k=1}^{l} g_k = 1$;

p_k – імовірність нападу на об'єкт;

$q_k(x, y)$ – імовірність виділення ресурсів x при заданому значенні y;

$f_k(x, y)$ – частка втраченої інформації на об'єкті.

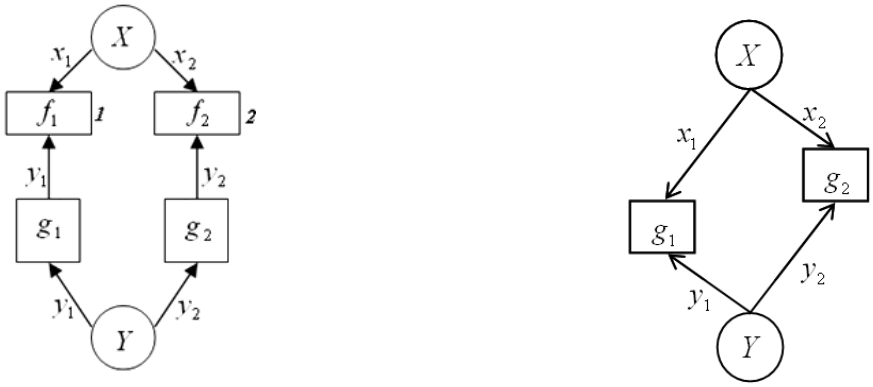
Величини, що входять в (1) – відносні: $i(x, y)$, $i_k(x, y)$, g_k віднесені до загальної вартості інформації, $f_k(x, y)$ – до вартості інформації на об'єкті. В позначеннях незалежних змінних індекси опущені.

Відповідно до моделі [3], вважаємо, що величина $f_k(x, y)$, котра виражає динамічну вразливість об'єкта, залежить від співвідношення ресурсів нападу і захисту. Крім того, приймемо, що при відсутності інвестицій у захист ($y = 0$) напад вилучає всю інформацію, котру покладемо рівною одиниці. Ще одна умова, яка накладається на функцію $f_k(x, y)$: при $x/y \to 0$ $f_k(x, y) \to 0$, при $x/y \to \infty$ $f_k(x, y) \to 1$. Найпростішою залежністю, котра задовольняє зазначеним умовам, є дробово-степенева функція:

$$f_k(x, y) = \frac{(x/y)^{n_k}}{(x/y)^{n_k} + c_k}, \qquad (2)$$

де параметри n_k і c_k визначають форму і крутизну залежностей.

Для ілюстрації методики розглянемо спрощену структуру інформаційної системи (рис.1,а), котра містить два об'єкти g_1, g_2, захищені індивідуальними перешкодами f_1 та f_2 (назви об'єктів одночасно визначають кількість інформації на них, а назви перешкод — вразливості об'єктів).



а **б**

Рис. 1. Схеми різних форм протистояння: а – однонаправленого; б – різнонаправленого

Параметри системи вважаємо відомими. Вразливості об'єктів на першому етапі описуються дробово-лінійними функціями: $n_1 = n_2 = 1$. Параметри c_k становлять: $c_1 = 32$, $c_2 = 128$. Розподіл інформації по об'єктах: $g_1 = 0.4$, $g_2 = 0.6$, що відповідає логічному рішенню – більша частина інформації розташована на об'єкті з меншою

вразливістю. Загальну кількість ресурсів нападу вважаємо сталою і задаємо рівною $X = 0.1$ (10% від вартості інформації).

Умову зворотної задачі сформулюємо наступним чином. Втрати інформації не повинні перевищувати $i_{гр} = 0.05$, загальні втрати – $S_{гр} = (i + Y)_{гр} = 0.09$. Необхідно знайти кількість ресурсів захисту Y і їх оптимальний розподіл $\{y_k^0\}$ по об'єктах, котрий забезпечує досягнення мінімального значення $S_{\min}$ при виконанні заданих обмежень і відповідає сідловій точці.

Розв'язок зворотної задачі зводимо до розв'язку прямої. Маючи на меті пошук сідлової точки, зосереджуємо увагу на таких складових цільової функції, як вразливість об'єктів $f_k(x, y)$ і розподіл інформації $\{g_k\}$. Для цього покладемо $p_k = 1$, $q_k(x, y) = 1$. Цільова функція при сформульованих умовах приймає вигляд:

$$(x, y) = i_1(x, y) + i_2(x, y) = 0.4\frac{x_1/y_1}{x_1/y_1 + 32} + 0.6\frac{x_2/y_2}{x_2/y_2 + 128}. \qquad (3)$$

Пошук сідлової точки ведемо шляхом почергової оптимізації розподілу ресурсів нападу і захисту, при чому ходи суперника вважаються відомими. Ця математична процедура відображає позиційну гру з відкритою інформацією. При відсутності сідлової точки ця процедура перетворюється в нескінченний циклічний процес, при її наявності досягається стаціонарний стан, котрий влаштовує обидві сторони. В системі (рис.1,а) при дробово-лінійній формі функцій вразливості сідлова точка існує при всіх значеннях параметрів [4].

Оптимальний розподіл ресурсів захисту при фіксованому розподілі ресурсів нападу $X = 0.1$ знаходимо з умови $S(y_1, y_2) \to \min$ при виконанні введених граничних обмежень на величини i, S. Результати розрахунків одержуємо з допомогою програмного комплексу MatLab. На рис.2, а, б представлено результати при дробово-лінійних функціях вразливості і цільовій функції у формі (3), на рис.2, в, г — при дробово-нелінійній функції вразливості одного з об'єктів і цільовій функції у вигляді:

$$i(x, y) = 0.4\frac{(x_1/y_1)^2}{(x_1/y_1)^2 + 256} + 0.6\frac{(x_2/y_2)^2}{(x_2/y_2)^2 + 128}.$$

Інтервал значень Y, в якому виконана умова $i \le i_{гр}$, на рис.2, а обмежений зліва точкою $Y_{гр}^{(1)} = 0.29$ (це точка А, що відповідає значенню $i_{гр} = 0.05$), справа – необмежений. Інтервал, який визначається умовою $S < S_{гр}$, де $S_{гр} = 0.09$, обмежується точками В і С. Перший із зазначених інтервалів позначимо правою косою штриховою, другий – лівою.

Перетин інтервалів, що представляє зону виконання обох граничних умов, обмежений точками А і С. Точка М, яка відповідає мінімуму залежності $S(Y)$, знаходиться всередині цієї зони і може бути прийнята за робочу. Кількість ресурсів захисту в точці М становить $Y = 0.04$, а оптимальний розподіл цих ресурсів за розрахунками: $y_1^0 = 0.024$, $y_1^0 = 0.016$. В точці М: $i = 0.04$, $S = 0.08$. Значення $Y = 0.04$ в робочій точці суттєво перевищує граничне значення $Y_{гр}^{(1)} = 0.029$, що створює певний запас надійності при реалізації режиму сідлової точки. Ще одна умова, яка висувається для забезпечення виконання заданих умов – незначне відхилення відношення y_1^0/y_2^0 в робочій зоні АС, котра займає інтервал $Y = 0.029..0.066$, від його оптимального

значення в робочій точці M. Ця умова виконується: на рис.2, б згадане відношення залишається незмінним і становить $y_1^0 / y_2^0 = 1.5$.

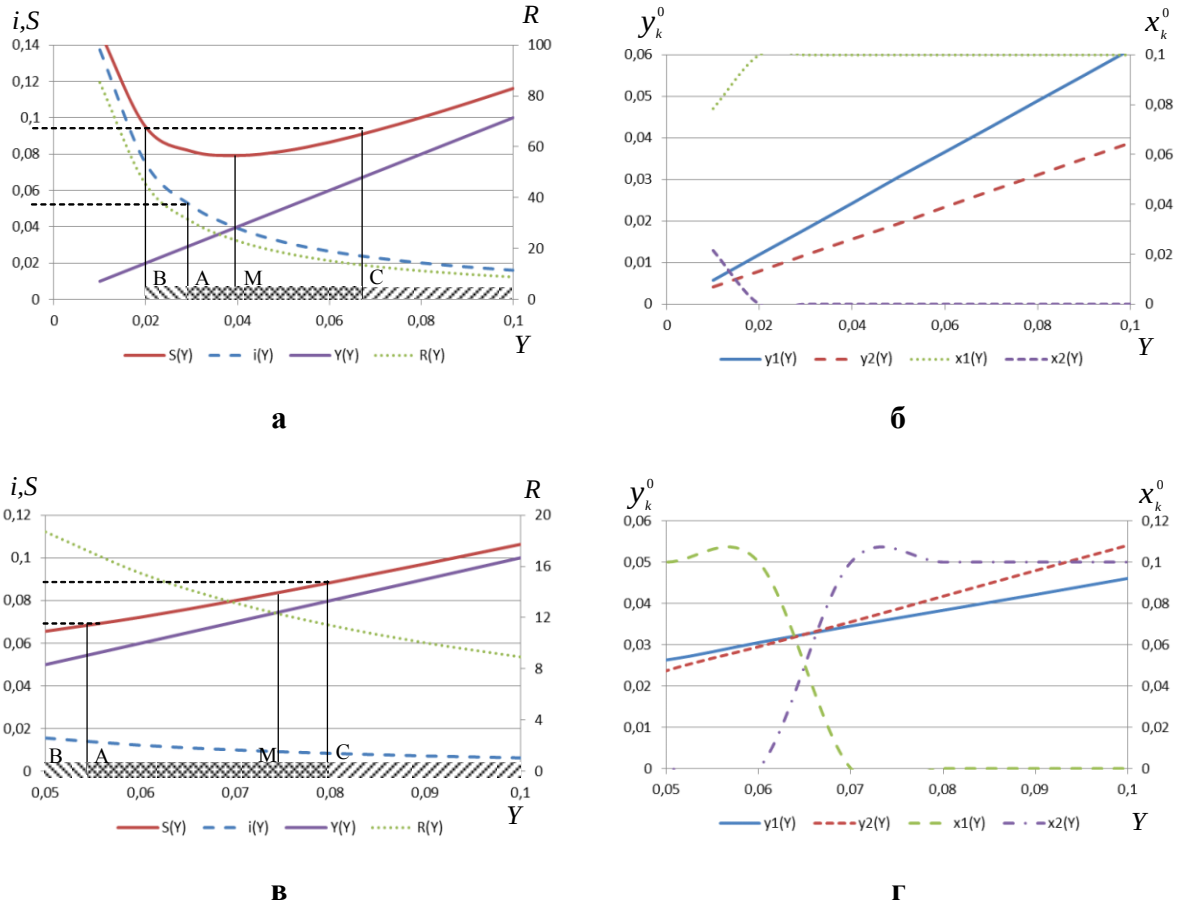


Рис. 2. Показники системи (рис.1, а) в сідлових точках при $g_1 = 0.4$, $g_2 = 0.6$: а – $n_1 = n_2 = 1$; $c_1 = 32$, $c_2 = 128$; б – $n_1 = n_2 = 1$; $c_1 = 32$, $c_2 = 128$; в – $n_1 = 2; n_2 = 1$, $c_1 = 256$, $c_1 = 128$; г – $n_1 = 2; n_2 = 1$, $c_1 = 256$, $n_2 = 128$

На рис.2, 3 наведено також залежності рентабельності $R(Y)$ інвестицій в захист інформації від розміру Y інвестицій. Рентабельність визначається як

$$R(Y) = \frac{b(Y)}{Y} = \frac{r(Y) - Y}{Y} = \frac{1 - i(Y) - Y}{Y},$$

де $r(Y)$ — дохід, $b(Y)$ — прибуток від внесення інвестицій. Зі зростанням витрат рентабельність зменшується, оскільки величина Y зростає швидше, ніж прибуток $b(Y)$. Звичайно, можлива постановка задачі, при якій обмеження встановлюється на величину рентабельності замість обмеження на $i(Y)$ чи $S(Y)$ або додатково до них.

Якщо хоч одна із залежностей $f_k(x, y)$ описується дробово-нелінійною функцією, то інтервал ΔY існування сідлової точки стає обмеженим [4]. Ширина інтервалу ΔY при сталому значенні X залежить від параметрів n_k, c_k функцій вразливості $f_k(x, y)$, а також від розподілу $\{g_k\}$. Може трапитись так, що мінімум залежності $S(Y)$ перебуває за межами цього інтервалу. Таку ситуацію спостерігаємо на рис.2 (в, г), де інтервал існування сідлової точки становить $\Delta Y = 0.05..0.1$. При рішенні

зворотної задачі поставимо умови: втрати інформації не повинні перевищувати $i_{гр} = 0.015$ (точка А, що відповідає значенню $Y = 0.055$), загальні втрати – $S_{гр} = 0.09$ (точка С з $Y = 0.08$). Інтервал АС, в якому виконується обидві умови, обмежений зліва першою умовою, а справа – другою і визначає зону допустимих значень $Y = 0.055..0.08$. Проте точка А, в котрій досягається найменше в інтервалі АС значення S, не може бути обрана робочою точкою, оскільки в ній не виконується умова забезпечення надійності реалізації заданих обмежень: по-перше, робоча точка повинна бути на деякому віддаленні від границі зони допустимих значень, по-друге, в околі робочої точки відношення y_1^0 / y_2^0 не повинно зазнавати кардинальних змін. Тому при виборі робочої точки слід дещо відступити від границі, а також врахувати залежності рис.2, г.

Зазначимо, що на рис.2, г порівняно з рис.2, б суттєво відрізняється хід розподілів ресурсів $\{x_k^0\}$, $\{y_k^0\}$ при зміні Y. На рис.2, б в робочій зоні всі ресурси нападника зосереджені на першому об'єкті $(x_1^0 = 0.1, x_2^0 = 0)$, а відношення y_1^0 / y_2^0 залишається незмінним і більшим одиниці. На рис.2, г така ситуація спостерігається лише при $Y \le 0.06$. В інтервалі $0.06 < Y < 0.07$ відбувається перекачка всіх ресурсів нападу на другий об'єкт, а для ресурсів захисту спостерігаємо їх поступовий перерозподіл і при $Y > 0.065$ маємо y_1^0 / y_2^0. З огляду на залежності рис.2, г робочу точку М обираємо при значенні $Y = 0.075$ (рис.2, в). В цій точці $i = 0.01$, $S = 0.082$, $y_1^0 = 0.036$, $y_2^0 = 0.039$. Зазначимо, що в зоні АС залежності $i(Y)$ та $S(Y)$ мають незначний нахил, і перехід від точки А до точки М не приведе до суттєвої зміни цих величин і погіршення показників.

Пояснимо вибір параметрів n_k, c_k в наших розрахунках. Параметр n_k виражає нелінійність функції вразливості $f_k(x, y)$, котра особливо проявляється в початковій області значень x/y. На рис.2, а, б функції вразливості для обох об'єктів — дробово-лінійні, на рис.2, в, г одна з цих функцій — дробово-квадратична. Параметр c_k впливає на висоту підйому залежності $f_k(x, y)$ над віссю абсцис. Вплив обох параметрів можна оцінити, порівнюючи значення $f_k(x, y)$ при одних і тих же значеннях x/y. Наприклад, при $x/y = 1$ і $n_k = 1$ функція (2) при $c = 32$ дає $f(x, y) = 0.03$ (3% втрат інформації), а при $c = 128$ — $f(x, y) = 0.08$ (0.8% втрат). Значення c_k в (3) обрані з умови забезпечення існування сідлової точки.

При ускладненні системи інформаційного протистояння, зокрема при переході до різнонаправлених дій кожної із сторін стають складнішими й умови досягнення режиму сідлової точки. На рис.1, б зображена система, в котрій сторона з ресурсами Y захищає інформацію на своєму об'єкті g_1 і прагне здобути інформацію суперника з об'єкту g_2, а сторона з ресурсами X захищає інформацію g_2 і прагне здобути інформацію g_1. В системі з двох об'єктів (рис.1, б) навіть при використанні дробово-лінійних функцій вразливості інтервал ΔY існування сідлової точки стає обмеженим, а режим існування сідлової точки досягається лише при певних значеннях параметрів, зокрема при рівномірному розподілі інформації між об'єктами: $g_1 = g_2$. Значення c_k впливають на розташування і ширину інтервалу ΔY. В наших розрахунках функції вразливостей мають вигляд:

$$f_1(x, y) = \frac{x/y}{x/y + 32}; \quad f_2(x, y) = \frac{x/y}{x/y + 64}.$$

Використані на рис.3 значення $c_1 = 32$, $c_2 = 64$ обрані з умови досягнення найбільшої ширини інтервалу: $\Delta Y = 0.12...0.17$. При двонаправленому протистоянні

втрати інформації на об'єктах захисту відображають лише одну частину протистояння і не можуть бути повноцінним показником. Таким показником для кожної з сторін є сумарний дохід $r(x,y)$, який включає дохід $i(x,y)$ від здобуття інформації суперника і дохід $j(x,y)$ від інвестицій в захист власної інформації, котрий визначаємо як різницю втрат при відсутності інвестицій і при їх внесенні:

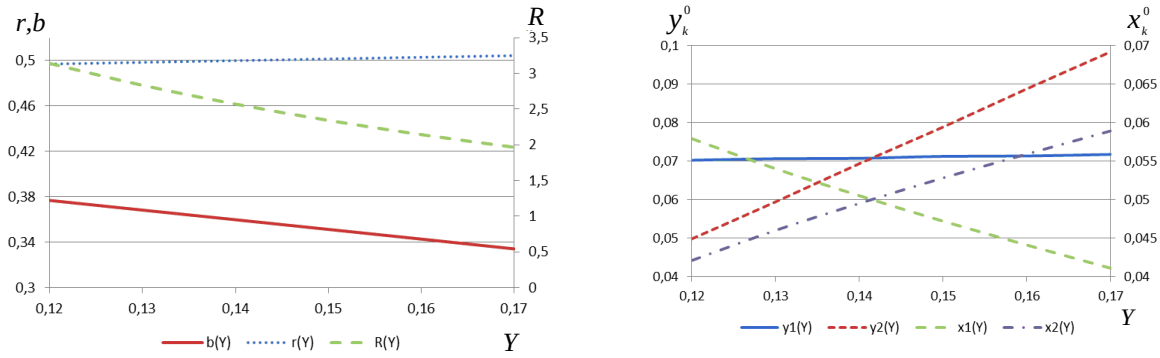
$$r_1(x,y) = j_1(x,y) + i_2(x,y) = g_1[1 - f_1(x,y)] + g_2 f_2(x,y), \tag{4}$$

$$r_2(x,y) = i_1(x,y) + j_2(x,y) = g_1 f_1(x,y) + g_2[f_2(x,y)]. \tag{5}$$

В останніх виразах $j_k(x,y)$ — частка загальної інформації g, захищена k-ю стороною на своєму об'єкті (ми покладемо $g = g_1 + g_2 = 1$), $i_k(x,y)$ — частка загальної інформації, здобута на об'єкті суперника. Цільові функції виражають прибутки обох сторін:

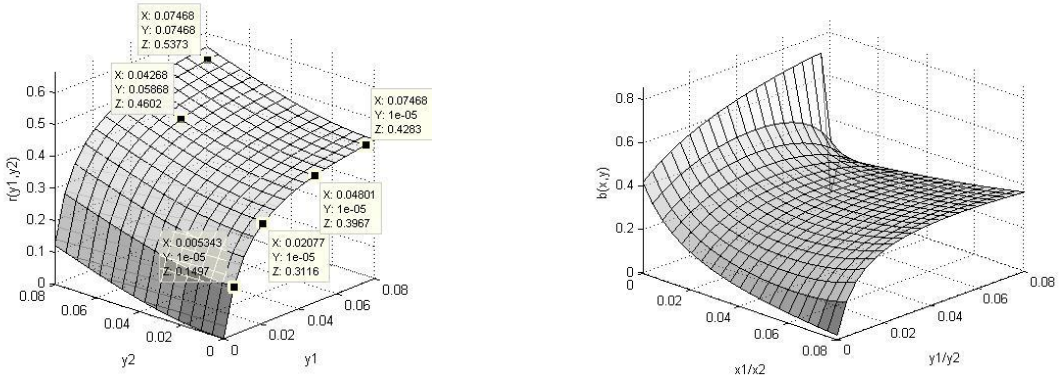
$$b_1(x,y) = r_1(x,y) - Y; \tag{6}$$

$$b_2(x,y) = r_2(x,y) - X. \tag{7}$$



а **б**

Рис. 3. Показники системи (рис.1, б) в сідлових точках при $g_1 = g_2 = 0.5$; $c_1 = 32$, $c_2 = 64$



а **б**

Рис. 4. Оптимальний розв'язок для системи (рис.1,б) в режимі сідлової точки: а – формування оптимального розв'язку при різних значеннях Y; б – поява сідлової точки при просторовому зображенні цільової функції

Критерієм оптимальності для сторін є досягнення максимуму функцій $b_k(x,y)$ (індекс k означає водночас номер сторони і номер об'єкта). Робочою точкою є точка одночасного досягнення максимуму функцій (6), (7). При геометричному зображенні результатів ця точка є вершиною куполоподібної фігури, побудованої на функціях $b_1(y)$, $b_2(x)$. Точку стаціонарності можна зобразити і у вигляді сідлової точки, перейшовши до двоїстої задачі, в якій необхідно досягти максимуму функції $b_1(y)$ і одночасно мінімуму цільової функції $b_1(x)$, котра визначає збитки другої сторони в результаті протистояння.

Графічну ілюстрацію розв'язку оптимізаційної задачі представлено на рис. 4. Максимальне значення величини $r(y_1, y_2)$ знаходимо в результаті перерізу вертикальної площини, котра проходить через лінію $y_1 + y_2 = Y$, з просторовою фігурою $r(y_1, y_2)$ при різних значеннях Y і сталому значенні X (рис.4, а). Графічне зображення сідлової точки на просторовій фігурі $r(x_1, x_2, y_1, y_2)$ дано на рис.4, б.

Розглядаючи дії сторони Y, задамось пошуком оптимальної кількості ресурсів $Y_{опт}$. Ситуація з визначенням $Y_{опт}$ схожа на ситуацію рис.2, в: оптимум цільової функції (в нашому випадку – максимум функції $b(Y)$) знаходиться за межами інтервалу існування сідлової точки, і робочу точку належить обирати з умови забезпечення надійності реалізації оптимального режиму. На рис.3,а максимальне значення $b_{\max}$ досягається на лівій межі інтервалу ΔY. Робоча точка повинна знаходитись на деякому віддаленні від цієї межі. Друга умова – відсутність різких змін відношення y_1^0 / y_2^0 в околі робочої точки — виконується в однаковій степені при всіх значеннях Y, оскільки залежності $y_1^0(Y)$ і $y_2^0(Y)$ близькі до лінійних. Обмеження, які покладались при односторонньому протистоянні на величини $i(Y)$ та $S(Y)$, в нашому випадку замінюють на вимогу досягнення максимальних значень прибутку і рентабельності. Оскільки обидві залежності $b(Y)$ і $R(Y)$ мають спадаючий характер і максимуму досягають на лівій границі інтервалу ΔY в точці $Y = 0.12$, то робочу точку М можна обрати при значенні $y^0 = 0.13$. В цій точці $b = 0.37$, $R = 0.47$, $y_1^0 = 0.07$, $y_2^0 = 0.06$.

Таким чином, для досягнення максимальних значень прибутку і рентабельності при надійній реалізації режиму сідлової точки в системі (рис.1,б) сторона Y повинна виділяти 13% від загальної вартості на обох об'єктах, причому ці ресурси слід розподілити в такій пропорції: 7% – на захист власної інформації на об'єкті g_1 і 6% – на здобуття інформації з об'єкту g_2. При цьому очікувані значення показників становлять: прибуток – 37% від загальної вартості інформації, рентабельність – 47% по відношенню до витрат на захист.

Як приклад реалізації описаного методу наведемо процес створення DLP системи для схеми (рис.1,а), показники якої зазначені на рис.2,а,б. Відповідно до вихідних умов маємо два об'єкти: два комп'ютери, на яких зберігається і обробляється інформація g_1 та g_2 загальною вартістю $g = g_1 + g_2 = 2762500$ грн. В точці М розподіл ресурсів по об'єктах, як зазначалось, становить $y_1^0 = 0.024$, $y_2^0 = 0.016$, або в абсолютних одиницях $\overline{y_1^0} = 65500$, $\overline{y_2^0} = 45000$. Опираючись на отримані дані, оберемо модулі системи (програми-агенти), які будуть встановлені на кожному з комп'ютерів: перший комп'ютер – {Mail-, IM-, Print-, Device-, HTTP-, Monitor-, File-, Programm- Sniffers}; другий комп'ютер – {Mail-, Skype-, HTTP-, FTP- Sniffers}. Використовуючи калькулятор для підрахунку вартості DLP системи, отримаємо: $\overline{y_1^0} = 65500$ грн., $\overline{y_2^0} = 45000$ грн. на рік. Сумарна вартість такої системи $Y = 110500$ грн.

Таким чином, при вартості інформації в 2762500 грн., система захисту для двох об'єктів буде коштувати 110500 грн. на рік і забезпечуватиме збереження 96% ($i = 0.04$) інформації навіть при оптимальному розподілі ресурсів нападником.

Слід звернути також увагу на те, що DLP система дає змогу оперативного керування програмами-агентами і «перекидати» їх між об'єктами. Саме за рахунок цієї особливості адміністратори СЗІ можуть в динамічному режимі впливати на вразливості перешкод.

Висновки

При пошуку оптимального рішення зворотної задачі слід зважати на те, що режим сідлової точки, котрий забезпечує деякий гарантований результат при будь-яких діях суперника, існує лише для певних структур і при певних умовах протистояння. Забезпечення існування цього режиму досягається шляхом вибору значень параметрів, котрі визначають вразливість об'єктів. Критерієм вибору робочої точки, котра визначає необхідну кількість ресурсів та їх розподіл між об'єктами, є забезпечення наступних показників: для одностороннього протистояння — мінімум загальних втрат, котрі об'єднують втрати інформації і витрати на її захист, при двосторонньому — максимум загального прибутку, який є сумою прибутку від внесення інвестицій в захист і прибутку від здобуття інформації суперника. Надійність реалізації оптимальної стратегії досягається за рахунок дотримання додаткових вимог: робоча точка повинна знаходитись на деякому віддаленні від межі інтервалу, в якому виконуються зазначені умови, і, крім того, в околі робочої точки не повинні спостерігатись значні зміни оптимального співвідношення ресурсів на об'єктах. Забезпечення наведених умов дозволяє визначити необхідні ресурси, а, зрештою, засоби захисту, що відкриває шлях до побудови оптимальних систем захисту інформації.

Список літератури

1. Глушак, В.В. Синтез структури системи захисту інформації з використанням позиційної гри захисника та зловмисника / В.В. Глушак, О.М. Новіков // Системні дослідження та інформаційні технології. — 2013. — №2. — С.89−100.
2. Демчишин, М.В. Графоаналітичний метод пошуку сідлової точки в ігрових задачах інформаційної безпеки / М.В. Демчишин, Є.Г. Левченко, Д.І. Рабчун // Системні дослідження та інформаційні технології. — 2014. — №3. С.48−61
3. Левченко, Є.Г. Оптимізаційні задачі менеджменту інформаційної безпеки / Є.Г. Левченко, А.О. Рабчун // Сучасний захист інформації. — 2010. — №1(1). — С.16−24
4. Левченко, Є.Г. Умови існування сідлової точки в багаторубіжних системах захисту інформації / Є.Г. Левченко, Р.Б. Прус, Д.І. Рабчун // Безпека інформації. — 2013. — №1. — С.70−76.

ПОИСК ОПТИМАЛЬНОГО РЕШЕНИЯ ОБРАТНОЙ ЗАДАЧИ ЭКОНОМИЧЕСКОГО МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е.Г. Левченко, Д.И. Рабчун

Национальный авиационный университет,
просп. Космонавта Комарова, 1, Киев, 03058, Украина; e-mail: professor_va@ukr.net

Первым шагом к синтезу систем защиты информации является решение обратной задачи, когда по заданным показателям системы находят необходимое количество ресурсов и их распределение между объектами. Рассмотрено информационную систему, которая содержит два объекта и может функционировать в двух режимах противостояния: однонаправленном, когда каждая сторона защищает свою информацию, и двунаправленном, когда каждая из сторон защищает свою информацию и стремится получить информацию соперника. Решение обратной задачи ввиду его сложности сводят к решению прямой и путем перебора, используя метод Беллмана, находят необходимые величины. Учитывая неопределенность условий противостояния в информационной сфере, необходимо найти такое решение, которое обеспечивает заданные показатели при любых действиях соперника. В экономической теории такая ситуация известна как равновесие по Нэшу. При геометрической интерпретации результатов она изображается седловой точкой на пространственной фигуре, которая представляет целевую функцию в зависимости от ресурсов обеих сторон. Найдем решение обратной задачи в интервалах существования седловой точки при различных значениях параметров системы. Установлены требования к параметрам, выполнение которых позволяет получить оптимальный результат.

Ключевые слова: информационная безопасность, математическая модель, распределение ресурсов, седловая точка.

SEARCH OF THE OPTIMAL SOLUTION OF THE INVERSE PROBLEM OF ECONOMIC MANAGEMENT OF INFORMATION SECURITY

E.G. Levchenko, D.I. Rabchu**n**

National Aviation University,
prosp. Kosmonavta Komarova, 1, Kyiv, 03058, Ukraine; e-mail: professor_va@ukr.net

The first step to the synthesis of information security systems is a solution of the inverse problem, when the system parameters are given the necessary amount of resources and their distribution between objects. We consider an information system which contains two objects and can work in two modes of confrontation: unidirectional, where each side protects the information and bidirectional when each side protects the information and aims to obtain the opponent's information. The solution of the inverse problem due to its complexity reduces to solving of direct problem with exhaustive search by using the method of Bellman. Taking into account the uncertainty of conditions of confrontation in the information area, it is necessary to find a solution which ensures the performance for any opponent's actions. In economic theory, such situation is known as Nash equilibrium. In a geometric interpretation of the results it is represented by saddle point on spatial figure which represents the objective function depending on the resources of both sides. We find solution of the inverse problem in the intervals of the existence of a saddle point for different values of the system parameters. We established requirements to parameters implementation of which allows you to get the best result.

Keywords: information security, mathematical model, distribution of resources, saddle point.