УДК 681. 324. 001: 681.3.004

Левченко Є.Г.

ОПТИМІЗАЦІЯ РОЗПОДІЛУ РЕСУРСІВ МІЖ ОБ'ЄКТАМИ ЗАХИСТУ ІНФОРМАЦІЇ

Розподіл обмежених ресурсів найефективнішим чином становить сутність економіки і одночасно зміст одного з напрямків дослідження операцій – галузі науки, яка займається розробкою методів оптимального управління організаційними системами [1, 2]. Такий підхід по відношенню до інформаційної безпеки приводить до постановки задачі оптимізації розподілу ресурсів між об'єктами захисту (ними можуть бути приміщення, носії інформації, лінії їх передач тощо).

Ця задача має декілька аспектів і потребує певних знань про ситуацію, які впливають на вибір методики розв'язку і кінцевий результат. До таких знань про кожний з об'єктів відносяться:

- кількість, якість і значущість інформації;
- природний і наявний рівень захищеності;
- кількість ресурсів, які може направити сторона (або сторони) нападу з врахуванням очікуваної імовірності події;
- кількість ресурсів, необхідних для достатньої захищеності;
- кількість ресурсів, які може виділити сторона захисту;
- допустимий рівень ризику втрати інформації.

Метою служби захисту інформації являється мінімізація можливостей її вилучення. Нападаюча сторона переслідує прямо протилежні цілі: розподіл своїх ресурсів, який створює максимальні можливості для її вилучення. Таким чином маємо протистояння двох сторін, що являється типовою задачею теорії ігор [3, 4].

Позначимо через x_k кількість ресурсів, вкладених стороною захисту (перший гравець), а через y_k --стороною нападу (другий гравець) в k-ий об'єкт ($k=1,2,\dots l$) і будемо вважати, що кількість вилученої інформації прямо пропорційна різниці $y_k - x_k$. Важливість кожного виду інформації характеризуємо ваговим коефіцієнтом g_k.

Функцією мети, наслідуючи методику військово-стратегічного планування [5], побудуємо у вигляді:

$$f(x,y)=\sum_{k=1}^{l}(y_k - x_k)g_k, \qquad (1)$$

$$\text{де } y_k - x_k = \begin{cases} y_k - x_k, \text{ при } y_k > x_k \\ \mathbf{0} \textbf{ при } y_k \le x_k \end{cases}$$

Добуток $f_k=(y_k - x_k)g_k$ визначає кількість інформації, вилученої з k-го об'єкту, з врахуванням її значущості. При $y_k - x_k \le 0$ кількість вилученої інформації дорівнює нулю.

Всі величини в правій частині виразу вважаємо нормованими.

При такій постановці задачі маємо матричну гру з нульовою сумою: виграти може тільки другий гравець, причому його виграш (вилучена інформація) дорівнює програшу, тобто від'ємному виграшу, першого (платіжна матриця цієї гри має негативний інгредієнт).

Поставимо себе на місце служби захисту інформації. Тоді нашою метою буде мінімізація функції $f(x,y)$. Розглянемо можливі варіанти розподілу ресурсів нападу y_k і підберемо розподіл ресурсів захисту x_k, який дозволяє досягти бажаного результату. Функція мети в цьому випадку матиме вигляд:

$$f_{ij}(x,y)=\sum_{k=1}^{l}(y_{jk}-x_{ik})g_k\,, \tag{2}$$

де x_{ik} і y_{jk} - кількість ресурсів, вкладених захистом і нападом в k-ий об'єкт при i-му варіанті розподілу ресурсів захисту (i=1,2,...m) і i-му варіанті розподілу ресурсів нападу (j=1,2,...n). Таким чином, під знаком суми стоїть інформація, вилучена з k-го об'єкту при ij-му варіанті розподілу ресурсів; в лівій частині – інформація, вилучена при цьому варіанті розподілу ресурсів з усіх об'єктів захисту.

Наше завдання - вибрати варіант розподілу ресурсів x_{ik}, який забезпечує мінімальне значення f_{ij} серед усіх можливих варіантів розподілу y_{jk}. Таким чином, ми зводимо розв'язок оберненої задачі до розв'язку прямої.

Звичайно, такий напівемпіричний підхід при невеликому числі пробних варіантів не може забезпечити оптимальність розподілу, хоча й може бути близький до нього (це залежить від того, наскільки вдало вибрані пробні варіанти розподілу x_{ik}). Першим з них (i=1) можна взяти розподіл x_{ik}, який повторює співвідношення $g_k - x_{11}:x_{12}:...:x_{1l}=g_1:g_2:...:g_l$ (тут мається на увазі, що вразливість об'єктів однакова; якщо це не так, то ступінь вразливості можна ввести в коефіцієнт g_k). Рухаючись методом послідовних наближень, ми можемо як завгодно щільно наблизитись до оптимального варіанта.

Спрощуючи задачу, розглянемо випадок, коли ресурси нападу не розпорошені по різних об'єктах, а зосереджені на якомусь одному з них (зазначимо, що концентрація ресурсів нападу в одному напрямку часто приносить кращі результати, ніж їх розподіл по різних об'єктах). В термінології теорії ігор це перехід від змішаної до чистої стратегії. В цьому випадку метою захисту являється мінімізація інформації, яку можна вилучити з одного об'єкта, і функцію мети записують у вигляді:

$$f_{ik}(x)=(Y-x_{ik})g_k\,, \tag{3}$$

де $Y=\sum_k y_k$ - сумарний ресурс нападу.

В умовах невизначеності поняття оптимальності не є однозначним. Оптимальний результат знаходиться по одному з відомих критеріїв [6], вибір котрого залежить від економічної позиції сторони захисту. Скористаємось критерієм Севіджа, який забезпечує мінімальний ступінь ризику вилучення інформації. Для кожного i-го варіанту розподілу x_{ik} знаходимо max f_{ik}, а потім з них вибираємо min max f_{ik}. Обраний критерій (критерій «мінімакса») встановлює граничне значення інформації, яка може бути вилучена при вкладанні всіх ресурсів нападу в один з об'єктів (при заданому співвідношенні g_k).

Розглянемо приклад. Пронормуємо вхідні дані до 1:

$X=\sum_k x_k=1$; $Y=\sum_k y_k=1$; $g=g_1+g_2+g_3=1$ і покладемо l=3;

$g_1=0{,}5$; $g_2=0{,}3$; $g_3=0{,}2$; $g_1:g_2:g_3=5:3:2$.

Розрахуємо значення функції мети (3) для декількох варіантів розподілу x_{ik} і одержані дані занесемо в таблицю 1, в якій також приведемо значення $\alpha_i=\max\limits_k f_{ik}$ і $\beta_k=\min\limits_i f_{ik}$. Число α_i є показник неефективності стратегії першого гравця (оскільки воно представляє максимальне значення вилученої інформації), а β_k - показник ефективності стратегії другого гравця [7].

З таблиці видно, що $\min\limits_i \alpha_i = \min\limits_i \max\limits_k f_{ik} = 0{,}195$ реалізується у варіанті i=3 при розподілі $x_{31} : x_{32} : x_{33} = 0{,}62 : 0{,}35 : 0{,}03$. Цей варіант гарантує, що кількість вилученої інформації не перевищить значення 0,195 (для порівняння: у варіанті i= 4 воно може бути 0,20, а у варіанті i=1 – 0,25).

Таблиця 1

$i \backslash k$		1	2	3	α_i
1	x_{1k} f_{1k}	0,5 0,25	0,3 0,21	0,2 0,16	0,25
2	x_{2k} f_{2k}	0,6 0,20	0,3 0,21	0,1 0,18	0,21
3	x_{3k} f_{3k}	0,62 0,19	0,35 0,195	0,03 0,194	0,195
4	x_{4k} f_{4k}	0,65 0,175	0,35 0,195	0,? 0,20	0,20
5	x_{5k} f_{5k}	0,7 0,15	0,2 0,24	0,1 0,18	0,24
β_k		0,15	0,195	0,16	

Для сторони нападу оптимальним являється варіант k=2 (всі ресурси вкладаються в другий об'єкт). В цьому варіанті кількість вилученої інформації буде не менше 0,195 при всіх розглянутих варіантах розподілу сил захисту (у варіанті k=1 вона може складати 0,15, а у варіанті k=3 - 0,16). Таким чином, третій рядок і другий стовпчик представляють оптимальні чисті стратегії для першого (сторона захисту) і другого (сторона нападу) гравців.

Оптимальні значення для обох сторін співпадають:

$$\min_i \max_k f_{ik} = \max_k \min_i f_{ik} = 0{,}195$$

і становлять ціну гри.

Якщо розглядати нашу задачу як скінченну гру, то цей результат відповідає теоремі Неймана про матричну гру двох партнерів з нульовою сумою і в геометричній інтерпретації зображається сідловою точкою на гіперповерхні $f(x,y)$.

Більш загальна постановка задачі передбачає наявність декількох джерел ресурсів захисту і декількох суб'єктів нападу. Схема розподілу ресурсів в цьому випадку зображена на рис. 1.

В цьому випадку математичне формування задачі являє собою систему лінійних нерівностей, які виражають обмеження, що накладаються на ресурси захисту і нападу:

$$\begin{aligned} &\sum_{k=1}^{l} x_{ik} \le X_i \qquad (i = 1, 2 \ldots m); \\ &\sum_{k=1}^{l} y_{jk} \le Y_j \qquad (j = 1, 2 \ldots n), \end{aligned} \tag{4}$$

Необхідно знайти розв'язок системи, який надає мінімуму функції мети, що виражає інформацію, вилучену з усіх об'єктів захисту всіма суб'єктами нападу:

$$f(x,y) = \sum_{j=1}^{n} \sum_{k=1}^{l} (y_{jk} - x_k) g_k \qquad - \min, \tag{5}$$

де $$x_k = \sum_{i=1}^{m} x_{ik};$$

$$(y_{jk} - x_k)g_k = \begin{cases} (y_{jk} - x_k)g_k & \text{- при } y_{jk} > x_k; \\ 0 & \text{- при } y_{jk} \le x_k. \end{cases}$$

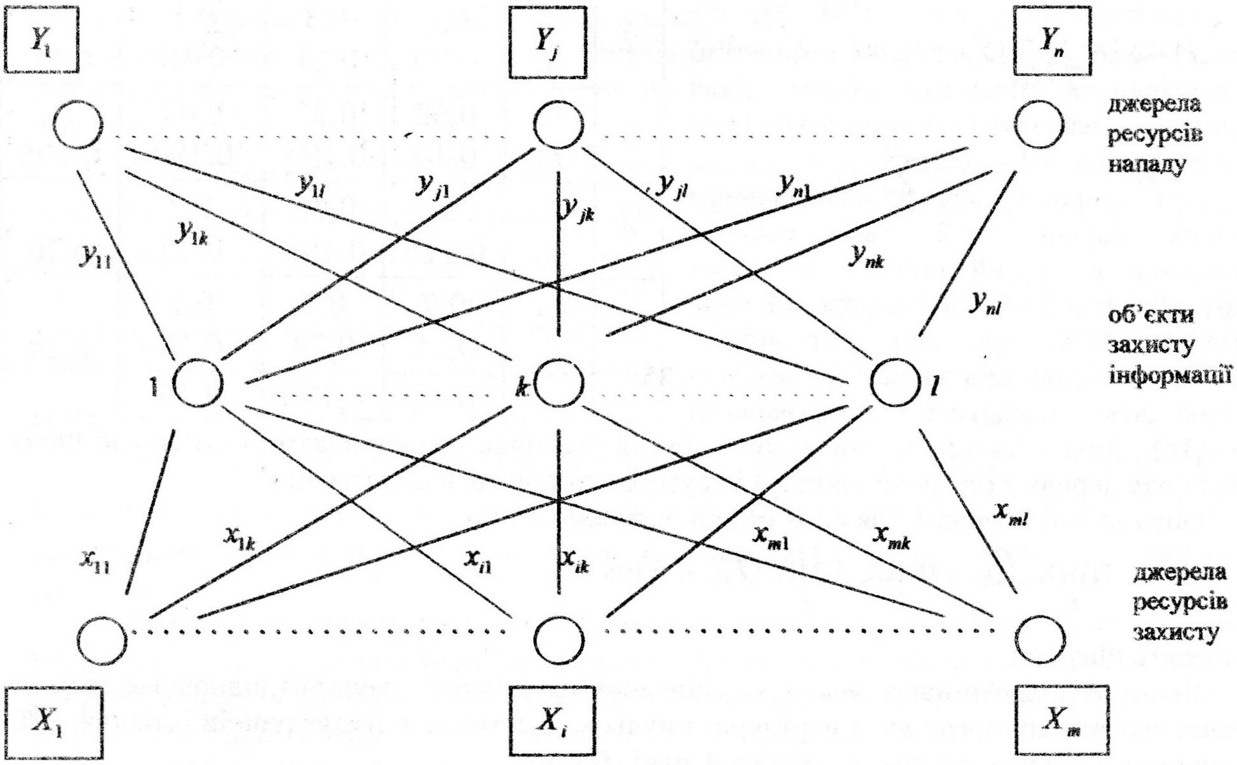

Рис. 1. Схема розподілу ресурсів за наявності декількох джерел ресурсів захисту і декількох суб'єктів нападу

В силу лінійності задачі вона може бути зведена до попередньої, коли ми мали одне джерело ресурсів захисту і один суб'єкт нападу і знаходити розв'язок (5) як суму таких частинних розв'язків.

Наступним кроком аналізу являється розгляд варіантів, які відрізняються співвідношеннями:

1) $z = \dfrac{Y}{X}$;

2) $Y_1 : Y_2 : \dots Y_n$;

3) $g_1 : g_2 : \dots g_l$,

а також вибором критерію оптимальності.

В такій постановці задачу можна розглядати, як аналіз змішаних стратегій, в якому роль ймовірностей грають вагові коефіцієнти g_k.

Розгляд нових варіантів приведе до розгалуження гілки рішень і пошуку нових критеріїв оптимальності, оскільки розподіл *x*, оптимальний по критерію (3) для $z_1 = \left(\dfrac{Y}{X}\right)_1$, вже не буде таким для $z_2 = \left(\dfrac{Y}{X}\right)_2$.

Проілюструємо це на прикладі. Проведемо аналогічні розрахунки чистих стратегій ще для двох значень $z = Y / X$: $z = 1.25$ і $z = 1.5$. Для $z = 1.25$ одержимо оптимальну чисту стратегію у вигляді $x_1 = 0.69; x_2 = 0.31; x_3 = 0$ з відповідними значеннями $f_1 = 0.280; f_2 = 0.282; f_3 = 0.250$. Для z = 1.5 – $x_1 = 0.75; x_2 = 0.25; x_3 = 0$ і $f_1 = 0.375; f_2 = 0.375; f_3 = 0.30$.

Ми діємо в умовах невизначеності як по відношенню до можливого об'єкту нападу (тобто значення *k*), так і по відношенню до можливих ресурсів нападу (значення *z*). Користуючись лапласівським підходом, будемо вважати прийняті нами значення *z* (як і значення *k*) рівноімовірними і ставити за мету мінімізацію f при всіх можливих значеннях *z*. Нашим завданням являється пошук розподілу x_k, який задовольняє поставленій умові. Обмежимось трьома варіантами розподілу x_k, які відповідають оптимальним стратегіям при $z = 1{,}0;\ 1{,}25;\ 1{,}5$ і виясними, якими будуть значення f_{kz} для кожного з цих розподілів при значеннях *z*, для яких відповідні стратегії не являються оптимальними.

Результати розрахунків представимо у вигляді таблиці 2 (виділені клітинки відповідають оптимальним чистим стратегіям).

Таблиця 2

i	*k*	x_k \ *z*	1.0	1.25	1.5	max f_{kz} *k, z*
1	1	0.62	[redacted]	0.32	0.44	
	2	0.35		0.27	0.35	0.44
	3	0.03		0.25	0.29	
2	1	0.69	0.155	[redacted]	0.41	
	2	0.31	0.207		0.36	0.41
	3	0	0.200		0.30	
3	1	0.75	0.125	0.25	[redacted]	
	2	0.25	0.150	0.30		0.375
	3	0	0.200	0.25		

З табл. 2 видно, що мінімакс $f_{kz} = 0.375$ досягається при розподілі x_k у співвідношенні 0,75:0,25:0, яке являється оптимальним для найбільшого з трьох можливих значень *z*: *z* = 1,5. Цілком зрозуміло, що при збільшенні *z* кількість вилученої інформації зростає.

Якщо є можливість оцінити імовірності дій сторони нападу, то одержаний результат можна уточнити. Позначимо імовірність нападу на *k*-ий об'єкт через p_k, а імовірність виділення для цієї мети ресурсів *z* стороннього нападу через q_z. Тоді вилучена інформація у відповідності з критерієм Байєса [7] буде визначатись функцією мети $F(p,q)$, яка для кожного i-го варіанту розподілу ресурсів x_{ik} сторони захисту розраховується як середнє зважене значень f_{kz} з врахуванням ймовірностей p_k, q_z:

$$F^{(i)}(p,q) = \sum_k \sum_z p_k f_{kz}^{(i)} q_z$$

або в матричній формі

$$F^{(i)}(p,q) = [p][f^{(i)}][q]^T$$

Приведемо деякі результати розрахунків на основі даних таблиці 3.

З попередніх розрахунків можна зробити висновок: розподіл x_{ik} слід вибрати таким, щоб він був оптимальним для максимально можливого значення $z = \frac{Y}{X}$ (в нашому випадку: $x_1 = 0.75, x_2 = 0.25, x_3 = 0$). Як видно з табл.3, значення $F^{(3)}$ являється мінімальним серед усіх $F^{(i)}$ при різних комбінаціях як , так і q_z. Зазначимо, що в (6) $f_{kz}^{(i)}$ - це показник чистих стратегій, $f_k^{(i)}$ - їх зважені середні значення з врахуванням імовірностей q_z.В теорії ігор z розглядається, як фактор „сил природи", зважаючи на непередбачуваність їх дій. В нашому випадку – це невизначеність, обумовлена недостатньою інформованістю про дії сторони нападу . $F^{(i)}(p,q)$ - можна розглядати як показник змішаної стратегії, поскільки це зважене середнє показників чистих стратегій $f_k^{(i)}$ з вагомими коефіцієнтами p_k. Оптимальним показником змішаних стратегій являється $\min F^{(i)}(p,q) = F^{(3)}(p,q) = 0.18$, який досягається при розподілі $x_1 : x_2 : x_3 = 0.75 : 0.25 : 0$.

Таблиця 3

p_1	0,5	0,5	0,4	0,4	0,7
p_2	0,3	0,3	0,35	0,35	0,2
p_3	0,2	0,2	0,25	0,25	0,1
q_1	0,6	0,4	0,4	0,2	0,6
q_2	0,3	0,4	0,4	0,35	0,3
q_3	0,1	0,2	0,2	0,45	0,1
$F^{(1)}$	0,24	0,28	0,26	0,29	0,24
$F^{(2)}$	0,23	0,25	0,25	0,29	0,22
$F^{(3)}$	0,18	0,23	0,23	0,27	0,20

Проведені розрахунки являються ілюстративними. Звичайно, поставлена задача повинна розв'язуватись методами лінійного програмування. Її математичне формування має такийкий вигляд:

$$F(p,q) \to \min$$

$$\sum_{k=1}^{l} x_{ik} \le X_i \, (i = 1,2...m); x_{ik} \ge 0;$$

$$\sum_{k=1}^{l} y_{jk} \le Y_j \, (j = 1,2...n); y_{jk} \ge 0$$

$$\sum_{k} p_k = \sum_{z} q_z = 1; p_k \ge 0; q_z \ge 0.$$

Використання пакета прикладних програм значно розширює множину можливих варіантів і спрощує процедуру пошуку оптимального рішення.

Список літератури

1. *Вентцель Е.С.* «Исследование операций». – М.: Дрофа, 2004.
2. *Шикин Е.В. Шикина Г.Е.* «Исследование операций». – М.: Проспект, 2006.
3. *Нейман Дж., Моргенштерн О.* «Теория игр и экономическое поведение». – М.: Л, 1960.
4. *Глухов В.В., Мечников М.Д., Коробко С.Б.* «Математические методы и модели менеджмента». –С-Пб.: Лань, 2005.
5. «Современная математика для инженеров», под редакцией Э. Беккенбаха. – М.: Издательство иностранной литературы,1959.
6. *Бланк И.А.* «Управление финансовыми рисками». – К.:Ника-центр, 2005.
7. *Лабскер Л. Г., Бабешко Л.О.* Игровые методы в управлении экономикой и бизнесом. М.: Дело, 2001.

Надійшла 29.11.2006 р.