зернових культур в Україні є тенденція до зростання та міжрічні коливання, причиною яких є біокліматичні фактори.

У статті побудовано та верифіковано прогнозовані моделі врожайності, які дозволяють оцінити зростання врожайності зернових у найближчі роки та відповідні перспективи продовольчого забезпечення і експортний потенціал України в цьому секторі.

Література

1. Програма «Зерно України — 2015». — К. : ДІА, 2011. — 48 с.
2. *Наконечний С.І.* Економетрія: підручник / Наконечний С.І., Терещенко Т.О., Романюк Т.П. — К. : КНЕУ, 2004. — 520 с.
3. *Грицюк П.М.* Аналіз, моделювання та прогнозування динаміки врожайності озимої пшениці в розрізі областей України : монографія. — Рівне : НУВГП, 2010. — 350с.
4. *Грицюк П.М.* Прогнозування врожайності зернових культур: особливості і методика // Вчені записки : зб. наук. праць. Вип. 11. — К. : КНЕУ, 2009. — С. 294-300.
5. *Грабовый П.Г.* Риски в современном бизнесе / П. Г. Грабовый. — М. : Аланс, 1994. — 292 с.
6. *Грицюк П.М.* Моделювання впливу метеофакторів на врожайність озимої пшениці // Вчені записки : зб. наук. праць. — К. : КНЕУ, 2010. — Вип. 12. — С. 216-224.
7. *Айвазян С.А.* Прикладная статистика. Основы эконометрики / С.А. Айвазян, В.С. Мхитарян. — М. : ЮНИТИ, 2001. — 1002 с.

УДК 336.761.6

Доценко С., к.ф.-м.н., доцент,
Київський національний економіний університет імені Вадима Гетьмана

МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЇ ЯК ІГРИ У ХОВАНКИ ТА ПОШУК

АНОТАЦІЯ. Як відомо, проблема захисту інформації є однією з найбільш актуальних і важливих завдань в інформації. Для того, щоб розглянути цю проблему всебічно, необхідно вибрати адекватні математичні моделі. Один із способів, щоб описати боротьбу. Той, хто уповноважений захищати конфіденційну інформацію в комп'ютерних мережах і той, хто намагається отримати несанкціонований доступ до нього є використання теорії ігор інструменти, а саме, так звані «хованки гри». Ці ігри включають в себе широкий спектр різних проблем і може бути коротко описана таким чином. Є два агента з протилежними інтересами. Один агент, який називається «Шкура», як правило, щось приховати, інший, який нази-

вається «шукач», як правило, щоб знайти об'єкт, захований в «Гітлера». Кілька моделей таких ігор висвітлені у статті. Пара оптимальних стратегій і Addle точки розміщені в кожному конкретному випадку.

ANNOTATION. As it well known, information protection problem is one of the most actual and important tasks in computer science. In order to consider this problem comprehensively, it's necessary to select the adequate mathematical models. One of the ways to describe the struggle of one, who is authorized to protect the confidential information at computer networks and one who is trying to get unauthorized access to it is to use game theory tools, namely, so-called «hide and seek games». These games include wide range of different problems and may be briefly described as follows. There are two agents with the opposite interests. One agent, who called «hider» tends to hide something, the other one, who called «seeker» tends to find the object, hidden by the «hider». A few models of such games are delivered at the article. A pair of optimal strategies and a addle point are found for each case.

Вступ. Розвиток сучасних мережевих технологій супроводжується підвищенням вимог до забезпечення конфіденційності обробки інформації та як наслідок — припускає істотну модернізацію стандартів керування інформаційною безпекою. Оскільки несанкціонований доступ до певних сегментів інформації стає привабливим для деяких осіб, то для забезпечення належного захисту інформації від їхніх посягань потребує вивчення їхніх методів і передбачення можливих вчинків. Подібно тому як криміналіст, який розкриває злочин, повинен ставити себе на місце злочинця, особа, яка розробляє системи захисту інформації, повинна ставити себе на місце особи, яка потенційно прагнутиме незаконно отримати цю інформацію.

Математичним апаратом моделей, у яких результат залежить не тільки від власних стратегій, але й від стратегій супротивника, є теорія ігор. Як добре відомо, теорія ігор ділиться на два класи — некооперативні (зокрема, антагоністичні) та кооперативні ігри. Антагоністичні ігри є ідеальним апаратом дослідження моделей першого типу, які можна охарактеризувати як напад-захист. Але розвиток комп'ютерних мереж призвів до того, що забезпечення інформаційної безпеки кожного з елементів мережі впливає на безпеку інших. Таким чином, виникає питання про те, що користувачі, які об'єднані у спільну мережу, повинні взаємодіяти з метою застосування спільної стратегії захисту мережі — це моделі другого типу. Апаратом дослідження таких взаємодій є кооперативна теорія ігор.

Дана стаття досліджує моделі першого типу, зокрема, розглядається кілька ігрових моделей ігор у хованки та пошук. При цьому мається на увазі, що захисник прагне сховати конфіденційну інформацію, а зловмисник — знайти її.

Проста гра у вгадування. Нехай гравець А вибирає будь-яке число від 1 до n, а В вгадує, яке число вибрав А. Нехай задано

набір додатніх чисел (a_1, a_2, …, a_n). Якщо А вибрав число k, а В вгадав вибір А, то А платить В суму a_k, а якщо ні, то ніяких виплат не відбувається. Зрозуміло, що А прагне мінімізувати, а В — максимізувати середню величину платні. Дана ігрова задача зводиться до матричної гри з діагональною матрицею *diag* (a_1, a_2, …, a_n). Очевидно, дана гра не має розв'язку в чистих стратегіях (або, іншими словами, платіжна матриця не має сідлової точки), отже, треба шукати її розв'язок у мішаних стратегіях.

Знайдемо мінімальний гарантований програш (МінГП) А проти будь-якої стратегії В. Нехай А дотримується мішаної стратегії (p_1, p_2, …, p_n). Якщо при цьому В дотримується своєї чистої k-ї стратегії, то середній програш А складає $p_k a_k$, а пошук стратегії, яка забезпечує МінГП, має вигляд:

$$\max(p_1 a_1,\ p_2 a_2, ...,\ p_n a_n) \to \min,\ p_i \geq 0,\ p_1 + ... + p_n = 1.$$

Дана величина досягає мінімуму у випадку, коли всі члени, які стоять під знаком максимуму, рівні між собою: $p_1 a_1 = p_2 a_2 = \ldots =$ $= p_n a_n$, звідси $p_k = \dfrac{(a_k)^{-1}}{\sum_{i=1}^{n} (a_i)^{-1}}$, а величина МінГП гравця А становитиме $\left(\sum_{i=1}^{n} (a_i)^{-1} \right)^{-1}$.

Аналогічно знайдемо максимальний гарантований виграш (МаксГВ) В проти будь-якої стратегії А. Нехай В дотримується мішаної стратегії (q_1, q_2, …, q_n). Якщо при цьому А дотримується своєї чистої k-ї стратегії, то середній виграш В складає $q_k a_k$, а пошук стратегії, яка забезпечує МаксГВ, має вигляд

$$\min(p_1 a_1,\ p_2 a_2, ...,\ p_n a_n) \to \max,\ q_i \geq 0,\ q_1 + ... + q_n = 1..$$

Дана величина досягає максимуму у випадку, коли всі члени, які стоять під знаком мінімуму, рівні між собою: $q_1 a_1 = q_2 a_2 = \ldots =$ $= q_n a_n$, звідси $q_k = \dfrac{(a_k)^{-1}}{\sum_{i=1}^{n} (a_i)^{-1}}$,, а величина МаксГВ гравця В становитиме $\left(\sum_{i=1}^{n} (a_i)^{-1} \right)^{-1}$.

Оскільки МінГП А та МаксГВ В збігаються, то знайдена величина $\left(\sum_{i=1}^{n}(a_i)^{-1}\right)^{-1}$ є ціною гри, а набори стратегій $(p_1, p_2, \ldots, p_n)$ та $(q_1, q_2, \ldots, q_n)$ (які в даному випадку збігаються між собою) утворюють сідлову точку.

Гра в охорону об'єкта. Нехай є n ящиків, в яких зберігаються задані грошові суми. Перенумеруємо ящики в спадному порядку цінностей $C_1 \geq C_2 \geq \ldots \geq C_n$. Нехай у грі беруть участь два гравці — злодій З та сторож С. Нехай С має можливість охороняти лише один ящик. Нехай З і С незалежно один від одного вибирають номер ящика. Якщо номери вибраних ящиків співпадають, то злодій не отримує нічого, в іншому разі він отримує величину C_i, де i — номер ящика, який вибрав злодій. Отже, З — прагне максимізувати, а С — мінімізувати величину вкраденого. На перший погляд, задача схожа на задачу про вгадування, яку було розглянуто раніше, однак, це не так. Якщо в попередньому випадку платіжна матриця мала діагональний вигляд (та завдяки цьому розв'язок гри знаходився легко), то в даному випадку на головній діагоналі платіжної матриці стоять нулі, а всі інші елементи додатні. Якщо стратегіям З відповідають рядки, а стратегіям С — стовпці, то платіжна матриця має вигляд

$$A = \begin{pmatrix} 0 & C_1 & \ldots & C_1 \\ C_2 & 0 & \ldots & C_2 \\ \ldots & \ldots & \ldots & \ldots \\ C_n & \ldots & C_n & 0 \end{pmatrix},$$

тому структура стратегій гравців буде відрізнятись від гри вгадування.

Спочатку знайдемо вигляд стратегії С, а потім вже й саму стратегію. Нехай С застосовує мішану стратегію $(p_1, p_2, \ldots, p_n)$, а З — свою i-ту чисту стратегію. Тоді виграш З складає $C_i(1 - p_i)$, і З буде вибирати таке i, щоб максимізувати цю величину. Тоді С, у свою чергу, повинен вибрати таку мішану стратегію, щоб мінімізувати величину

$$\max(C_1(1-p_1), C_2(1-p_2), \ldots, C_n(1-p_n)). \qquad (1)$$

Для того щоб зрозуміти вигляд стратегії С, доведемо ряд допоміжних лем.

Позначимо $N = 1, \ldots, n$. Нагадаємо, що спектром мішаної стратегії $(p_1, p_2, \ldots, p_n)$ (позначається Sp) називається множина всіх індексів j, для яких $p_j > 0$.

Лема 1. Спектр оптимальної стратегії С складається з двох або більшої кількості чистих стратегій.

Доведення. Нехай вираз (1) досягає мінімуму для деякої чистої стратегії j, тобто $p_j = 1$, $p_i = 0$, $i \neq j$. Позначимо через M множину індексів, для яких досягається $\max\limits_{i \in N/j} C_i$. Тоді можна перейти до другої мішаної стратегії С, вибираючи деяке мале Δ, збільшуючи для всіх $j \in M$ значення p_j з нуля на Δ та зменшивши величину p_j на $|\mathrm{M}| \cdot \Delta$, де $|\mathrm{M}|$ — кількість елементів у множині M, що призведе до зменшення (1), а це суперечить припущенню про те, що для даної стратегії С $(p_1, p_2, \ldots, p_n)$ вираз (1) досягає мінімуму.

Лема 2. Нехай при змішаній стратегії $(p_1, p_2, \ldots, p_n)$ вираз (1) досягає мінімуму. Тоді $\max\limits_{j \in Sp} C_j(1-p_j) \geq \max\limits_{j \in N/Sp} C_j$.

Доведення. Нехай $\max\limits_{j \in Sp} C_j(1-p_j) \geq \max\limits_{j \in N/Sp} C_j$ (2).

Позначимо через M множину всіх індексів, для яких досягається максимум правої частини (2). Тоді можна перейти до іншої мішаної стратегії С, вибираючи деяке мале Δ, збільшуючи для всіх $j \in M$ значення p_j з нуля на Δ та зменшуючи для деякого $j \in Sp$ величину p_j на $|\mathrm{M}| \cdot \Delta$, що призведе до зменшення (1), що суперечить припущенню про те, що для даної стратегії С $(p_1, p_2, \ldots, p_n)$ вираз (1) досягає мінімуму.

Лема 3. Нехай при мішаній стратегії $(p_1, p_2, \ldots, p_n)$ вираз (1) досягає мінімуму. Тоді $(\forall j, i \in Sp)(C_i(1-p_i) = C_j(1-p_j))$.

Доведення. Припустимо супротивне. Нехай $M \subset Sp$, $K \subset N/Sp$ — множини індексів, на яких досягається максимум виразу (1). Згідно з припущенням леми, множина М не збігається зі Sp. Отже, існує такий індекс $i \in Sp/M$, що $C_i(1-p_i) < C_j(1-p_j) = \underset{j \in M}{} \underset{k \in K}{C_k}$. У силу леми 2, $C_k < C_i(1-p_i)$. Тоді можна перейти до другої мішаної стратегії С, вибираючи деяке мале Δ, збільшити на Δ значення p_j для всіх $j \in M \cup K$, зменшивши при цьому значення p_j на $|M \cup K| \cdot \Delta$, що призведе до зменшення (*), що суперечить припущенню про те, що для даної стратегії С $(p_1, p_2, \ldots, p_n)$ вираз (1) досягає мінімуму.

Лема 4. Нехай при мішаній стратегії $(p_1, p_2, \ldots, p_n)$ вираз (1) досягає мінімуму. Тоді спектр цієї стратегії має вигляд $1, \ldots, k$, при цьому $C_{k+1} < C_k$.

Доведення. Припустимо супротивне, тобто що спектр стратегій розривний, тобто існує деякий індекс і такий, що $i \in Sp$, $(i-1) \notin Sp$.

Тоді, з одного боку, оскільки встановлено нумерацію в спадному порядку C_j, то $C_{i-1} \geq C_i$, а з другого боку, завдяки лем 2, 3 справедливий ланцюг нерівностей $C_{i-1} \leq \max\limits_{j \in N/Sp} C_j \leq \max\limits_{j \in Sp} C_j(1-p_j) = = C_i(1-p_i) < C_i$.

Таким чином, оптимальна стратегія С має вигляд (p_1, p_2, …, p_k, 0, …, 0), де k — мінімальний індекс, для якого $C_1(1-p_1) = = C_2(1-p_2) = \ldots = C_k(1-p_k) \geq C_{k+1}$, звідси $p_i = \dfrac{\sum\limits_{j=1}^{k}\left(\dfrac{1}{C_j}\right) - \dfrac{k-1}{C_i}}{\sum\limits_{j=1}^{1}\dfrac{1}{C_j}}$, $i \leq k$, $p_i = 0$, $i > k$, де k — мінімальний індекс, для якого справедлива нерівність $k-1 \geq C_{k+1}\left(\dfrac{1}{C_1}+\ldots+\dfrac{1}{C_k}\right)$, або $k = n$, якщо нерівність не виконується ні для яких значень k. Дотримуючись знайденої мішаної стратегії, С гарантує, що його програш складе не більш, ніж $V = C_i(1-p_i)_{\forall i \leq k} = \dfrac{k-1}{\sum\limits_{j=1}^{k}\dfrac{1}{C_j}}$ при будь-якій стратегії З. Точніше, це буде в точності V, якщо З буде грати будь-яку з чистих стратегій, що належить знайденому спектру 1, …, k або ж їхню будь-яку ймовірнісну суміш і це буде величина, менша від V, якщо З вийде за межі спектра 1, …, k.

Оскільки $V \geq C_{k+1}$, то набір стратегій З слід шукати у вигляді (r_1, r_2, …, r_k, 0, …, 0), при чому, згідно теореми про активні стратегії, він має застосувати таку активну стратегію, щоб С було байдуже, який саме ящик (з 1-го по k-й) охороняти. Це означає, що середній виграш З, рівний $(C_1r_1 + \ldots + C_kr_k) - C_ir_i$ не повинен залежати від i, $i = 1, k$. Це досягається тоді і тільки тоді, коли значення C_ir_i попарно рівні для всіх $i = 1, k$.

Звідси $r_i = \dfrac{\dfrac{1}{C_i}}{\sum\limits_{j=1}^{1}\dfrac{1}{C_j}}$, $i \leq k$, $r_i = 0$, $i > k$.

Отже, дотримуючись такої мішаної стратегії, З гарантує собі виграш не менший від V при будь-якій стратегії С. Точніше, це

буде в точності V, якщо С буде грати будь-яку з чистих стратегій, що належать знайденому спектру 1, …, k або будь-яку їхню ймовірнісну суміш, і це буде величина, менша від V, якщо С вийде за межі спектру 1, …, k.

Таким чином, дана пара стратегій З і С утворюють сідлову точку з ціною гри V.

Приклад. Нехай $n = 4$, $p_1 = 4$, $p_2 = 3$, $p_3 = 2$, $p_4 = 1$.

Для $k = 2$: $(k = 2) - 1 < \left(\frac{1}{4} + \frac{1}{3}\right) \cdot 2$,

для $k = 3$: $(k = 3) - 1 > \left(\frac{1}{4} + \frac{1}{3} + \frac{1}{2}\right) \cdot 1$, отже

$$p_4 = 0,\ S = \frac{1}{4} + \frac{1}{3} + \frac{1}{2} = \frac{13}{12},\ p_1 = \frac{S - \frac{2}{4}}{S},\ p_2 = \frac{S - \frac{2}{3}}{S},\ p_3 = \frac{S - \frac{2}{2}}{S},$$

$$\vec{p} = \left(\frac{7}{13}, \frac{5}{13}, \frac{1}{13}, 0\right).$$

$$r_1 = \frac{1/4}{S};\quad r_2 = \frac{1/3}{S};\quad r_3 = \frac{1/2}{S};\quad r_4 = 0,\quad \vec{r} = \left(\frac{3}{13}, \frac{4}{13}, \frac{6}{13}, 0\right),$$

$$V = \frac{(k = 3) - 1}{S} = \frac{24}{13}.$$

Гра у хованки та багатократний пошук з необмеженим часом у пошукувача. У даній грі бере участь два гравці, а саме той, хто ховається (позначимо його H — від слова hider), і той, хто шукає (позначимо його S — від слова searcher). Нехай H ховає предмет в один із n ящиків. Гравець S відкриває ящики до тих пір, доки не знайде захований предмет. Час, необхідний для відкриття i-го ящика задано та дорівнює t_i. При цьому припускається, що S має необмежений час на пошук, але при цьому прагне мінімізувати середній час пошуку. H прагне так сховати предмет, щоб максимізувати середній час пошуку гравцем S.

Для $n = 2$ задача зводиться до біматричної гри з симетричною платіжною матрицею:

$$C = \begin{pmatrix} t_1 & t_1 + t_2 \\ t_1 + t_2 & t_2 \end{pmatrix}.$$

Оскільки всі $t_i > 0$, то очевидно дана гра не має сідлової точки. Оскільки в даному випадку обидві стратегії гравців є активними,

то розв'язок гри в мішаних стратегіях легко знаходиться з теореми про активні стратегії. Нехай (p_1, p_2) — оптимальна мішана стратегія Н, тоді значення ціни гри не повинно залежати від того, який стовпець вибере Н, звідси

$$p_1t_1 + p_2(t_1 + t_2) = p_1(t_1 + t_2) + p_2t_2, \text{ отже, } p_1 = \frac{t_1}{t_1 + t_2},\ p_2 = \frac{t_2}{t_1 + t_2},$$

а ціна гри — $V = p_1t_1 + p_2(t_1 + t_2) = \dfrac{t_1^2 + t_2^2 + t_1t_2}{t_1 + t_2}$.

Далі, аналогічно частинному випадку $n = 2$, наведемо оптимальні стратегії гравців і ціну гри для довільного n та покажемо методом математичної індукції, що наведені формули є правильними.

Оптимальною стратегією H буде мішана стратегія, яка полягає в тому, щоб сховати предмет в i-й ящик з імовірністю $\dfrac{t_i}{\sum_{j=1}^{n} t_j}$, $i = 1, n$.

Оптимальною стратегією S буде мішана стратегія вибору послідовності проглядання ящиків, яку можна задати за допомогою наступного алгоритму.

Нехай з самого початку множина S складається із всіх індексів $i = 1, n$.

Номер чергового ящика вибираємо з S з імовірністю $\dfrac{t_i}{\sum_{j\in S} t_j}$, і якщо предмет буде знаходитись не в даному ящику, то викреслюємо індекс i з множини S і знову таким самим чином розігруємо номер наступного ящика для проглядання. Формально це означає, що якщо σ — деяка перестановка індексів від 1 до n, σ(i) — позиція індексу i в цій перестановці, то S повинен проглядати ящики в порядку, який задається перестановкою σ з імовірністю

$$p_\sigma = \prod_{i:\sigma(i)=1,n-1} \frac{t_i}{\sum_{j:\sigma(j)\geq\sigma(i)} t_j}.$$

При цьому ціна гри виявляється рівною

$$V(t_1, ..., t_n) = \frac{\sum_{i=1}^{n} t_i^2 + \sum_{i \neq j} t_i t_j}{\sum_{i=1}^{n} t_i}.$$

Зазначимо, що всі наведені формули є вірними для $n = 2$. Припустимо, що формули є вірними для n і покажемо, що вони є вірними для $n + 1$.

Нехай для випадку $n + 1$ гравець Н дотримується мішаної стратегії $\left(\frac{t_1}{\sum_{i=1}^{n+1} t_i}, ..., \frac{t_{n+1}}{\sum_{i=1}^{n+1} t_i} \right)$. Покажемо, що дана стратегія дає середній час пошуку $V(t_1, \ldots, t_{n+1})$ для будь-якого порядку проглядання S, що задається довільною перестановкою. Нехай першим елементом в цій перестановці буде $n + 1$. Тоді середній час пошуку складає

$$t_{n+1} + \left(1 - \frac{t_{n+1}}{\sum_{i=1}^{n+1} t_i} \right) \cdot V(t_1, ..., t_n) = t_{n+1} + \frac{\sum_{i=1}^{n} t_i}{\sum_{i=1}^{n+1} t_i} \cdot \frac{\sum_{i=1}^{n} t_i^2 + \sum_{i,j,i \neq j}^{1,n} t_i t_j}{\sum_{i=1}^{n} t_i} =$$

$$= \frac{t_{n+1} \sum_{i=1}^{n+1} t_i + \sum_{i=1}^{n} t_i^2 + \sum_{i,j,i \neq j}^{1,n} t_i t_j}{\sum_{i=1}^{n+1} t_i} = \frac{\sum_{i=1}^{n+1} t_i^2 \sum_{i,j,i \neq j}^{1,n+1} t_i t_j}{\sum_{i=1}^{n+1} t_i} = V(t_1, ..., t_{n+1}).$$

Якщо ж S починає проглядання не з елемента $n + 1$, а з іншого довільного елементу, то доведення того, що середній час проглядання складає $V(t_1, \ldots, t_{n+1})$ після перенумерації індексів буде аналогічним. Оскільки знайдена стратегія H дає час проглядання $V(t_1, \ldots, t_{n+1})$ при будь-якому порядку проглядання, який задає гравець S, тоді таким самим буде середній час проглядання при будь-якій мішаній стратегії S.

Аналогічно зазначаємо, що якщо гравець S дотримується своєї оптимальної мішаної стратегії, то ціна гри не залежить від того, в якому саме ящику ховає предмет гравець H. Таким чином, знайдена пара стратегій гравців S і H утворює сідлову точку з ціною гри $V(t_1, \ldots, t_{n+1})$.

Приклад. Нехай є три ящики з часами проглядання 1, 2 і 3 одиниці часу.

Тоді гравець А повинен застосувати мішану стратегію $\left(\frac{1}{6}, \frac{2}{6}, \frac{3}{6}\right)$.

Знайдемо ймовірності, з якими В повинен вибирати перестановки, які задають порядок проглядання:

$$(1,2,3) — \frac{1}{1+2+3}\frac{2}{2+3} = \frac{2}{30},\ (1,3,2) — \frac{1}{1+3+2}\frac{3}{3+2} = \frac{3}{30},$$

$$(2,1,3) — \frac{2}{2+1+3}\frac{1}{1+3} = \frac{2}{24},\ (2,3,1) — \frac{2}{2+3+1}\frac{3}{3+1} = \frac{6}{24},$$

$$(3,1,2) — \frac{3}{3+1+2}\frac{1}{1+2} = \frac{1}{6},\ (3,2,1) — \frac{3}{3+2+1}\frac{2}{2+1} = \frac{2}{6}.$$

Ціна гри (тобто середній час пошуку предмета) дорівнює

$$V = \frac{1^2 + 2^2 + 3^2 + 1\cdot 2 + 1\cdot 3 + 2\cdot 3}{1+2+3} = \frac{25}{6}.$$

Гра у хованки та багатократний пошук з обмеженим часом у пошукувача. Нехай H може сховати предмет в один з n ящиків, і нехай час пошуку в i-му ящику складає t_i. Нехай у S на пошук є час T, такий, що $\max(T_i) \le T < \sum T_i$, і таким чином у S достатньо часу, щоб відкрити будь-який з ящиків, але недостатньо, щоб відкрити всі ящики одразу. Метою H є мінімізувати, а метою S — максимізувати ймовірність знаходження предмета.

Нехай $N = \{1, \ldots, n\}$. Назвемо множину $M \subset N$ максимальною, якщо S може проглянути всі елементи множини M і при цьому не може додатково проглянути жодного елементу, тобто

$$\sum_{i\in M} t_i \le T, (\forall j \in N \setminus M)\left(\sum_{i\in M}(t_i) + t_j > T\right).$$

Тоді мішаною стратегією S буде ймовірнісна суміш вибору однієї з своїх максимальних підмножин, дана задача зводиться до матричної гри, розв'язок якої у свою чергу зводиться до пари задач лінійного програмування.

Розглянемо матрицю A, яка складається з 0 та 1, рядкам якої відповідають максимальні множини (стратегії S), а стовпцям — номера ящиків (стратегії H). Будемо вважати, що елемент A_{ij} рівний 1, якщо множина M_i містить індекс j та 0 в іншому випадку.

Тоді виходить, що S та H грають в матричну гру, в якій S вибирає рядки, а H-стовпці. Позначимо $I = (1, \ldots, 1)^T$ — вектор-стовпець, який складається з одиниць. Тоді пара двоїстих задач лінійного програмування має вигляд

S	H
$V \to \max$ $A^T\vec{q} \geq V\vec{I}$ $\vec{q} \geq 0, (\vec{q}, \vec{I}) = 1$	$V \to \min$ $A^T\vec{q} \leq V\vec{I}$ $\vec{q} \geq 0, (\vec{q}, \vec{I}) = 1$

Приклад. Нехай $N = \{1, \ldots, 5\}$, $t_i = i$, $T = 6$. Тоді існує чотири максимальних множини $M_1 = \{5,1\}$, $M_2 = \{4,2\}$, $M_3 = \{4,1\}$, $M_4 = \{3,2,1\}$, і матриця А має вигляд

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Іноді матрична гра може спрощуватись за домінуванням. У даному разі 1-й стовпець слабо домінує 5-й, а 2-й — 3-й, тому можна викреслити 1-й і 2-й стовпці. З точки зору теорії ігор викреслювання домінуючих стовпців і домінованих рядків у матричній (антагоністичній) грі не впливає на ціну гри. При цьому, якщо множина рівнозначних оптимальних стратегій для вихідної матричної гри складається з більш, ніж одного елементу, то вона може звужуватись, але при цьому обов'язково розв'язок матричної гри для перетвореної матриці відповідає розв'язку для вихідної матриці.

Стосовно даної задачі пошуку, спрощення платіжної матриці відповідає таким міркуванням H: «якщо я виберу 1-й ящик, то S знайде предмет, якщо вибере стратегії M_1, M_3 або M_4, а якщо 5-й — то тільки M_1, тому завжди замість 1-го ящика слід вибирати 5-й, гірше від цього не буде». Таким чином, ймовірність вибору 1-го ящика в оптимальній стратегії H дорівнює нулю, що відповідає викресленню 1-го стовпця. Аналогічно, порівнюючи 2-ї та 3-ї стратегії, викреслюємо 2-й стовпець.

Після спрощення платіжна матриця набуває вигляд:

$$S_1 = \{5,1\} \qquad \begin{matrix} 3 & 4 & 5 \end{matrix}$$
$$S_2 = \{4,2\} \qquad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$
$$S_3 = \{4,1\}$$
$$S_4 = \{3,2,1\}$$

Для перетвореної матриці стратегії S_2 та S_3 для S стають рівнозначними. Після їх об'єднання в одну стратегію матриця гри звелася до одиничної.

Таким чином, оптимальною стратегією H є ховати предмет в 3-й, 4-й або 5-й ящик з ймовірностями 1/3. Оптимальною стратегією S є застосування мішаної стратегії, в якій S_1 та S_4 вибираються з ймовірностями 1/3, а S_2 та S_3 можна змішувати в будь-якій пропорції, але так, щоб сума ймовірностей їхнього вибору складала 1/3.

Література

1. *Мазалов В.В*. Математическая теория игр / В. В. Мазалов. — СПб.: Лань, 2010. — 446 с.
2. *Петросян Л.А*. Теория игр / Петросян Л.А., Зенкевич Н.А., Шевкопляс Е.В. — СПб. : БХВ-Петербург, 2012. — 432 с.
3. *M. Osborne*. A course on game theory / M. Osborne, A. Rubinstein // The MIT Press, 1994. — 352 p.

УДК 336.1.0018

Бабинюк О. І., асистент
кафедри комп'ютерної математики та інформаційної безпеки ФІСІТ,
Київський національний економічний університет імені Вадима Гетьмана

ЗАСТОСУВАННЯ МЕТОДІВ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Щоб думку ворога дізнатися, серця розкривають,
а не те що листи.
У. Шекспір «Король Лір»

АНОТАЦІЯ. Викладено етапи розвитку становлення криптографічного захисту інформації. Висвітлено проблеми захисту даних в інформаційних системах і проблеми розподілу ключів у криптографії. Розглянуто