УДК 004.056.5

В.М. Безштанько, Я.В. Зінченко

МЕТОДИ РОЗВ'ЯЗАННЯ ЛІНІЙНИХ ДІОФАНТОВИХ РІВНЯНЬ В ЗАДАЧАХ МОДЕЛЮВАННЯ ПРОЦЕСІВ В КОМПОНЕНТАХ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Визначено процес управління ризиками як елемент системи управління інформаційної безпеки, а також методики оцінки рівня ризиків. Запропоновано підхід до кількісної оцінки ризиків на основі постановки задачі у вигляді діофантового рівняння. Проведено аналіз відомих методів розв'язання лінійних діофантових рівнянь, які застосовуються в процесі моделювання ризиків і їх оцінок. Отримано результати, які дозволяють накласти на досліджувану модель обмеження, що, у свою чергу, дозволяє здійснити перехід від розгляду нескінченної множини розв'язків до розв'язку задачі перебору з допустимою кількістю розглядуваних варіантів.

Ключові слова: система управління інформаційної безпеки, аналіз ризиків, діофантове рівняння.

Вступ

Одним з основних елементів системи управління інформаційної безпеки (СУІБ) організації є процес управління ризиками, для визначення рівня яких відповідними стандартами пропонується використання якісної, кількісної або комбінованої методик оцінки ризиків.Застосування даних методик дає можливість проведення детального аналізу джерел загроз для активів, а також визначення фінансових витрат, які необхідні для вибору мір захисту інформації[1, 2].

Серед зазначених вище найбільш складним і трудомістким єпроцескількісноїоцінкиризиків безпеки інформації, тому вданій роботі пропонується підхід до моделювання оцінок ризиків на основі постановки задачі у вигляді діофантового рівняння, що, на думку авторів, дозволить спростити хід даного процесу.

Постановка задачі

Нехай a – це розмір збитків, x – "частота" їх виникнення.Тоді для одного активу можна записати наступне співвідношення для оцінки ризику:

$$a \cdot x = r\,. \tag{1}$$

Значення прийнятного ризику r в кожній організації встановлюється індивідуально, а розмір збитків a може бути визначений експертними методами. Величина ж x повинна визначатися на основі статистичних даних про кількість інцидентів і на початковому етапі оцінки ризиків, як правило, є невідомою. Якщо a і r відомі, то співвідношення (1) можна розглядати як рівняння з одним невідомим відносно x. В цьому випадку знаходження x не викликає труднощів. Однак для стабільного розвитку організації важливим є виконання умови, коли значення сумарних ризиків $\sum_{j=1}^{n} a_j x_j$ не перевищує прийнятного значення $r_{\max}$:

$$\sum_{j=1}^{n} a_j x_j \le r_{\max}\,, \tag{2}$$

щопризводить до необхідності розв'язувати рівняння з n невідомими виду:

$$a_1 x_1 + a_2 x_2 + \ldots + a_j x_j = r\,. \tag{3}$$

В реальних ситуаціях допускається оцінка розміру збитків a_j і величини ризику $r_{\max}$ з точністю до цілих чисел. Якщо "частоту" x_j оцінювати в цілих відсотках, то співвідношення

(3) можна трактувати як діофантове рівняння відносно x_j. Враховуючи, що рівняння (3)або не має розв'язків,або має нескінченну множину розв'язків,реалізація обмеження (2) повинна забезпечуватися за рахунок виконання деяких додаткових умов.Зокрема, такі умови можуть бути наслідком обмеження на розв'язання рівняння (3) у множині додатних цілих чисел Z_+ .Згідно [3, 4] задача цілочислового розв'язання лінійного діофантового рівняння в області додатних чисел є *NP*-повною,а в деяких випадках – *overNP*-повною задачею. Однак у випадку відносно невеликої кількості невідомих у рівнянні (3) і наявності результативних обмежень на його розв'язання,виконання повного переборуна сучасній обчислювальній техніціє цілком можливим.

Основна частина

Відомо, що для розв'язання рівняння (3) в Z_+ необхідне виконання таких умов [5, 6]:

1. Рівняння виду (3), де $a_j \in Z_+$, $x_j \in Z$, $r \in Z_+$ має розв'язок в цілих числах тоді, коли найбільший спільний дільник d чисел $a_1, a_2, \ldots, a_j$ є дільником числа r. Таким чином: $r = d \cdot t$, де t – деяке ціле число. Як наслідок: якщо деякі цілі числа $x_1, x_2, \ldots, x_j$ задовольняють рівнянню (3), то d буде дільником кожного добутку чисел $a_1x_1, a_2x_2, \ldots, a_jx_j$, а також дільником їх суми r. Тобто d є дільником рівняння (3).

2. Якщо $d > 1$, то при перетворенні рівняння (3) до $d = 1$ кількість розв'язків і їх значення не зміняться, а коефіцієнти $a_1, a_2, \ldots, a_j$ перетворяться у відповідні взаємно-прості числа.

3. Для існування $d > 1$ рівняння виду (3) треба щоб r не було простим числом.

4. Із пунктів 1 і 3 випливає, що якщо r – просте число, то для існування цілочислового розв'язку рівняння (3) необхідно щоб найбільший спільний дільник d чисел $a_1, a_2, \ldots, a_j$ дорівнював одиниці.

5. Для існування цілочислового розв'язку рівняння (3) в області додатних чисел необхідне також виконання умови: $r \geq (a_1 + a_2 + \ldots + a_j)$.

6. Рівняння виду (3) має розв'язки в області додатних цілих чисел при $r > \prod_{j=1}^{n} a_j$.

Проведемо аналіз відомих методів розв'язання лінійних діофантових рівнянь (ЛДР) з урахуванням викладених вище обмежувальних умов. Спочатку розглянемо методи для двох невідомих:

$$a_1x_1 + a_2x_2 = r. \tag{4}$$

Методи розв'язання ЛДР для двох невідомих

Метод 1.

Припустимо, що рівняння (4) має окремий розв'язок $\{x_1', x_2'\}$. Отримане рівняння $a_1x_1' + a_2x_2' = r$ віднімемо від рівняння (4). Запишемо рівняння у такому вигляді: $a_1(x_1 - x_1') + a_2(x_2 - x_2') = 0$. Відповідно $a_1(x_1 - x_1') = -a_2(x_2 - x_2')$, $(x_1 - x_1') = \dfrac{-a_2(x_2 - x_2')}{a_1}$.

З отриманого співвідношення випливає, що $(x_1 - x_1')$ буде цілим числом за умови, якщо $(x_2 - x_2')$ ділиться націло на a_1. Тобто можна записати: $x_2 - x_2' = a_1t$, де $t \in Z$ (множині цілих чисел). Тоді: $\begin{cases} x_1 = x_1' - a_2t \\ x_2 = x_2' + a_1t \end{cases}$, де $t \in Z$.

Для отримання цілочислового додатного результату необхідне виконання додаткових умов: $a_2 t < x_1'$ та $a_1 t < x_2'$.

Приклад. Розв'яжемо рівняння:

$$4x_1 + 3x_2 = 54. \quad (5)$$

Нехай для рівняння (5) за допомогою генетичного алгоритму [7] знайдено окремий розв'язок – пара чисел $x_1' = 9$ та $x_2' = 6$. Тоді загальний розв'язок для даного рівняння можна записати у вигляді: $\begin{cases} x_1 = 9 - 3t \\ x_2 = 6 + 4t \end{cases}$, де $t \in Z$. Отже, для даного прикладу: $-3t < -9$ та $4t < -6$, або $-1{,}5 < t < 3$.

У відповідності з уведеним раніше обмеженням $x_j \in Z_+$, коефіцієнт t може набувати значень $\{-1, 0, 1, 2\}$. Тоді розв'язками рівняння (5) будуть пари чисел $\{12, 2\}, \{9, 6\}, \{6, 10\}, \{3, 14\}$. Інтерпретація цих розв'язків – це пари значень "частоти" величин $\{x_1, x_2\}$, а саме: 12% і 2%, 9% і 6%, 6% і 10%, 3% і 4%. Вибір конкретної пари значень повинен диктуватися контекстом оцінювання ризику, який є у експериментатора.

Метод 2.

Припустимо, що у рівнянні (4) коефіцієнти підлягають умові $a_2 < a_1$. Тоді розв'яжемо це рівняння відносно невідомого, при якому коефіцієнт найменший, тобто відносно x_2. Після виконаних перетворень отримаємо: $a_2 x_2 = r - a_1 x_1$, $x_2 = \dfrac{r - a_1 x_1}{a_2}$.

Приклад. Розв'яжемо рівняння (5). Почнемо відносно змінної x_2, оскільки в неї менший коефіцієнт. Після виконаних необхідних перетворень отримаємо: $x_2 = \dfrac{54 - 4x_1}{3}$. Для дотримання умови $x_j \in Z_+$ необхідно щоб $54 - 4x_1 > 0$, тобто $-4x_1 > -54$, $x_1 < 13{,}5$. Підставляючи в отриманому виразі замість x_1 довільні додатні цілі числа знаходимо цілочислові значення x_2. Якщо $x_1 = 1$, то $x_2 = \dfrac{54-4}{3} = \dfrac{50}{3}$; якщо $x_1 = 2$, то $x_2 = \dfrac{54-8}{3} = \dfrac{46}{3}$; якщо $x_1 = 3$, то $x_2 = \dfrac{54-12}{3} = \dfrac{42}{3} = 14$ і т.д. В результаті розв'язками рівняння будуть пари чисел $\{3{,}14\}$, $\{6{,}10\}$, $\{9, 6\}$, $\{12, 2\}$.

При застосуванні даного методу вводяться додаткові обмеження, а саме: $r - a_1 x_1 > 0$, $r - a_1 x_1$ повинне націло ділитися на a_2.

Метод 3.

Розв'язання ЛДР ґрунтується на властивостях найбільшого спільного дільника d. Для розв'язання рівняння (4) використовується алгоритм Евкліда.

Припустимо, що $a_1 > a_2$. Розділивши коефіцієнти a_1 на a_2 з лишком будемо мати: $a_1 = a_2 q_1 + n_1$, $a_2 = n_1 q_2 + n_2$, $n_1 = n_2 q_3 + n_3$. Також отримаємо:

$$n_{n-1} = n_n \, q_n. \quad (6)$$

Представимо найбільший спільний дільник n_3 коефіцієнтів a_1 і a_2 в лінійному вигляді [8]:

$$n_3 = n_1 + (-q_3)n_2 = n_1 + (-q_3)(a_2 + (-q_2)n_1) = a_1 + (-q_1)a_2 + (-q_3)(a_2 + (-q_2)(a_1 + (-q_1)a_2)) = a_1 + (-q_1) \times$$

$$\times a_2 + (-q_2)(-q_3)a_1 + (-q_3)(-q_2)(-q_1)a_2 + (-q_3)a_2 .$$

В результаті отримаємо лінійне представлення d коефіцієнтів a_1 і a_2, тобто представлення найбільшого спільного дільника у вигляді: $(a_1, a_2) = a_1 u + a_2 v$, де u і v – коефіцієнти Безу. Вони, у свою чергу, можуть бути представлені у вигляді: $u = 1 + (-q_2)(-q_3)$, $v = -q_1 + (-q_3)(-q_2)(-q_1) + (-q_3)$.

Розв'язки рівняння (4) можна представити як: $\begin{cases} x_1 = x_1' - vt \\ x_2 = x_2' + ut \end{cases}$, де $t \in Z$; $\{x_1', x_2'\}$ – є окремим розв'язком рівняння.

Приклад. Розв'яжемо рівняння (5). По формулі (6) знайдемо d коефіцієнтів (4, 3): $4 = 3 \times 1 + 1$, $3 = 1 \times 3 + 0$. Запишемо його лінійне представлення: $(4, 3) = 1 \times 4 + (-1) \times 3$. Знайдемо окремий розв'язок рівняння: $\begin{cases} x_1' = ur = 1 \times 54 = 54; \\ x_2' = vr = (-1) \times 54 = -54 \end{cases}$, де $u = 1$, $v = -1$. Запишемо його загальний розв'язок: $\begin{cases} x_1 = 54 - 3t \\ x_2 = -54 + 4t \end{cases}$, де $t \in Z$.

Для знаходження прийнятних значень "частоти" виникнення збитків необхідно щоб x_1 та x_2 набували цілочислових додатних значень. В наведеному прикладі це можливо якщо $54 - 3t > 0$ і $-54 + 4t > 0$. Відповідно $3t < 54$, $4t > 54$, $13{,}5 < t < 18$. Отже $t \in Z_+$. При $t = \{14, 15, 16, 17\}$ розв'язками рівняння (5) будуть наступні пари чисел: $\{12, 2\}$, $\{9, 6\}$, $\{6, 10\}$, $\{3, 14\}$.

Узагальнюючи результат,що показаний у прикладі, можна сформулювати наступні додаткові обмеження для діапазону шуканих значень "частот" виникнення збитків в запропонованій моделі: $\frac{r}{a_1} < t < \frac{r}{a_2}$, де $t \in Z$, а $a_1 > a_2$.

Метод 4.

Рівняння (4) розв'язується методом ланцюгового дробу. Розв'язок $\{x_1, x_2\}$ знайдемо у вигляді: $\begin{cases} x_1 = x_1' + x_1'' \\ x_2 = x_2' + x_2'' \end{cases}$, де $\{x_1', x_2'\}$ – окремий розв'язок рівняння (4), а $\{x_1'', x_2''\}$ – окремий розв'язок рівняння виду:

$$a_1 x_1 + a_2 x_2 = 0 . \qquad (7)$$

Представимо коефіцієнти a_1 та a_2 рівняння (4) у вигляді ланцюгового дробу [9]. Нехай $a_1 > a_2$, тоді дріб $\frac{a_1}{a_2}$ запишемо у вигляді суми цілої частини і правильного дробу: $\frac{a_1}{a_2} = \frac{a_2 q_0 + n_0}{a_2} = q_0 + \frac{1}{\frac{a_2}{n_0}} = q_0 + \frac{1}{\frac{q_1 n_0 + n_1}{n_0}} = q_0 + \frac{1}{q_1 + \frac{1}{\frac{n_0}{n_1}}} = \ldots\ldots = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \ldots . \frac{1}{q_n}}}$, де q_n – неповна частка, а n_n – лишки з алгоритму Евкліда. Також для перетворення раціонального числа до виду ланцюгового дробу можна скористатися згаданим вище алгоритмом Евкліда.

Якщо при побудові ланцюгового дробу зупинитися на знаменнику q_n, то отримаємо необхідний дріб $[q_0, q_1, q_2 .... q_n]$, який позначають $\frac{P_n}{Q_n}$.

Знайдемо вид деяких підходящих дробів: $\frac{P_0}{Q_0} = \frac{q_0}{1}$, $\frac{P_1}{Q_1} = q_0 + \frac{1}{q_1} = \frac{q_0 q_1 + 1}{q_1}$, $\frac{P_2}{Q_2} = q_0 + \frac{1}{q_1 + \frac{1}{q_2}} = \frac{q_2(q_0 q_1 + 1) + q_0}{q_2 q_1 + 1} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0}$.

Для раціонального числа $\frac{a_1}{a_2}$ послідовність підходящих дробів скінчена і її останній елемент $\frac{P_n}{Q_n} = \frac{a_n}{a_{n+1}}$. Чисельник і знаменник $(n+1)^{-q}$ дробу можна обчислити за формулами: $P_{n+1} = q_{n+1} P_n + P_{n-1}$, $Q_{n+1} = q_{n+1} Q_n + Q_{n-1}$. Чисельник і знаменник пов'язані між собою наступним співвідношенням: $P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1}$.

Усі підходящі дроби нескорочувані, а останній підходящий дріб співпадає по значенню з раціональним числом $\frac{P_n}{Q_n} = \frac{a_1}{a_2}$, де $d\ (a_1, a_2) = 1$. Тоді:

$$a_1 Q_{n-1} - a_2 P_{n-1} = (-1)^{n-1}. \tag{8}$$

Помножимо рівність (7) на $(-1)^{n-1} r$. Отримаємо: $a_1 \left(Q_{n-1} (-1)^{n-1} r\right) - a_2 \left(P_{n-1} (-1)^n r\right) = r.$

В якості окремого розв'язку рівняння (4) візьмемо: $x_1' = Q_{n-1}(-1)^{n-1} r$, $x_2' = P_{n-1}(-1)^n r$.

Використовуючи метод 1 для розв'язання рівняння (7) маємо: $\begin{cases} x_1'' = a_2 t \\ x_2'' = -a_1 t \end{cases}$, де $t \in Z$.

Таким чином, можна стверджувати, що розв'язок рівняння (4) буде мати вигляд: $\begin{cases} x_1 = x_1' + x_1'' = Q_{n-1}(-1)^{n-1} r + a_2 t \\ x_2 = x_2' + x_2'' = P_{n-1}(-1)^n r - a_1 t \end{cases}$, де $t \in Z$.

Приклад. Розв'яжемо рівняння (5). Перетворимо у ланцюговий дріб коефіцієнти: $\frac{4}{3} = \frac{3 \cdot 1 + 1}{3} = 1 + \frac{1}{\frac{3}{1}} = 1 + \frac{1}{\frac{3 \cdot 1 + 0}{1}} = 1 + \frac{1}{3 + \frac{1}{0}} = [1,3]$. Коефіцієнти дорівнюють: $\frac{P_0}{Q_0} = \frac{1}{1}$, $\frac{P_1}{Q_1} = \frac{q_0 q_1 + 1}{q_1} = \frac{4}{3}$. Отже: $\begin{cases} x_1' = Q_{n-1}(-1)^{n-1} r = 1 \cdot (-1)^0 \cdot 54 = 54 \\ x_2' = P_{n-1}(-1)^n r = 1 \cdot (-1)^1 \cdot 54 = -54 \end{cases}$. Окремими розв'язками рівняння (5) будуть: $\begin{cases} x_1'' = 3t \\ x_2'' = -4t \end{cases}$. Підставляючи дані вирази в (6) отримаємо результат: $\begin{cases} x_1 = x_1' + x_1'' = 54 + 3t \\ x_2 = x_2' + x_2'' = -54 - 4t \end{cases}$, де $t \in Z$.

Для знаходження прийнятних значень "частоти" виникнення збитків $\{x_1, x_2\}$ в області додатних значень необхідно щоб $54 + 3t > 0$, відповідно $3t > -54$, або $t > -18$. Також

$-54-4t>0$, відповідно $4t<-54$, або $t<-13{,}5$. Тобто, для отримання цілочислових додатних значень x_1 та x_2 в моделі оцінки ризиків необхідно щоб $-18<t<-13{,}5$. При $t=\{-14,-15,-16,-17\}$ розв'язками рівняння (5) будуть наступні пари чисел: $\{12,2\}$, $\{9,6\}$, $\{6,10\}$, $\{3,14\}$.

Для рівняння (4) можливе введення додаткових обмежень: $-\frac{r}{a_2}<t<\frac{r}{a_1}, a_1>a_2$.

На практиці аналіз ризиківдля активів проводиться в СУІБ, яка складається більше ніж з двох компонент. З цього випливає необхідність аналізу методів розв'язання ЛДР, що містять $n>2$ невідомих. Припустимо, що аналізуються ризики в системі, яка складається з трьох активів. Для такої системи можна записати діофантове рівняння з $n=3$ виду:

$$a_1x_1+a_2x_2+a_3x_3=r. \tag{9}$$

Проаналізуємо методи розв'язання цього рівняння.

Методи розв'язання ЛДР для трьох невідомих

Метод 1.

На практиці при формуванні моделі кількісного аналізу ризиків може виникнути ситуація, коли значення розміру збитків a_1,a_2,a_3 приблизно однакові, тобто $a_1\approx a_j$. Припустимо, що $a_1=a_2$. Також запишемо: $x_1+x_2=y$. Тоді рівняння (9) буде мати наступний вигляд:

$$a_1y+a_3x_3=r. \tag{10}$$

Розв'язавши рівняння будь-яким методом для двох невідомих отримаємо y. Відповідно отримаємо $x_2=y-x_1$.

Приклад. Нехай коефіцієнти розміру збитків a_1,a_2,a_3 приймають цілочислові додатні значення $\{4,4,3\}$, прийнятний ризик $r=54$. Необхідно знайти прийнятні значення "частоти" виникнення збитків для недопущення перевищення ризиків.

Запишемо рівняння:

$$4x_1+4x_2+3x_3=54. \tag{11}$$

Припустимо, що $x_1+x_2=y$. Тоді рівняння (11) можна записати наступним чином:

$$4y+3x_3=54. \tag{12}$$

Скориставшись будь-яким методом розв'язання ЛДР для двох невідомих отримаємо окремі розв'язки рівняння (12) – пару чисел $\{3,14\}$. Далі визначимо значення змінної x_2: $x_2=y-x_1=3-x_1$. Підставляючи замість x_1 значення $\{1,2\}$ отримаємо значення для x_2 –пару чисел $\{2,1\}$. Отже, розв'язком рівняння (11) будуть числа $\{1,2,14\}$ або $\{2,1,14\}$.

Для отримання множини розв'язків рівняння (11) його треба розв'язувати використовуючи всі окремі розв'язки рівняння (12). При розв'язанні рівняння (9)для отримання цілочислових додатних розв'язків крім обмежень, які існують для методу розв'язання рівняння (12) при $n=2$, необхідно враховувати й таке обмеження: $y>x_1,x_2$.

Метод 2.

Серед коефіцієнтів a_1, a_2, a_3 рівняння (9) виберемо найменший. Припустимо, що $a_1 < \{a_2, a_3\}$. Розділимо a_2 і a_3 на a_1 з лишком. Отримаємо: $a_2 = q_2 a_1 + w_1$, $a_3 = q_3 a_1 + w_2$, де $0 \le w_1 < a_1$ і $0 \le w_2 < a_2$.

Підставимо отримані вирази в рівняння (9). Отримаємо: $a_1 x_1 + (q_2 a_1 + w_2) x_2 + + (q_3 a_1 + w_3) x_3 = r$ або:

$$a_1(x_1 + q_2 x_2 + q_3 x_3) + w_2 x_2 + w_3 x_3 = r. \quad (13)$$

Нехай $y_1 = x_1 + q_2 x_2 + q_3 x_3$, $y_2 = x_2$, $y_3 = x_3$. Тоді рівняння (13) можна записати наступним чином: $a_1 y_1 + w_2 y_2 + w_3 y_3 = r$. Процес його перетворення має такі властивості:

– отримане рівняння або має меншу кількість змінних, або менші коефіцієнти при них;

– якщо хоч один з лишків w_2, w_3 перетвореного рівняння дорівнює нулю, то кількість змінних зменшується.

Відповідно для рівняння (13): $x_1 = y_1 - q_2 x_2 - q_3 x_3$, $x_2 = y_2, x_3 = y_3$.

Оскільки послідовність натуральних чисел, які зменшуються, не може бути нескінченною, то будемо мати або рівняння з одним невідомим, або рівняння, в якому усі коефіцієнти a_1, a_2, a_3 будуть однаковими.

Приклад. Розв'яжемо рівняння:

$$2x_1 + 3x_2 + 4x_3 = 54. \quad (14)$$

Розділимо 4 і 3 на 2 з лишком. Отримаємо: $4 = 2 \cdot 2 + 0$, $3 = 1 \cdot 2 + 1$. Підставимо отримані числа в рівняння (14) і запишемо: $2(x_1 + x_2 + 2x_3) + 1 \cdot x_2 + 0 \cdot x_3 = 54$.

Нехай $y_1 = x_1 + x_2 + 2x_3$ і $y_2 = x_2, y_3 = x_3$. Тоді отримаємо:

$$2y_1 + y_2 = 54. \quad (15)$$

Розв'яжемо рівняння (14) відносно змінної y_1. Тоді отримаємо: $y_1 = \dfrac{54 - y_2}{2}$.

Нехай окремим розв'язком рівняння (14) будуть числа $y_1 = 26$ та $y_2 = 2$. Із виразу $y_1 = x_1 + x_2 + 2x_3$ знайдемо $x_1 = 26 - x_2 - 2x_3$.

Нехай $x_2 = y_2 = 2$. Тоді $x_1 = 26 - 2 - 2x_3$ або:

$$x_1 + 2x_3 = 24. \quad (16)$$

Запропонованим вище методом 1 для $n = 2$ розв'яжемо рівняння (16). Отримаємо: $\begin{cases} x_1 = 10 - 2t \\ x_3 = 7 + t \end{cases}$, де $t \in Z$, а окремим розв'язком рівняння буде пара чисел $\{10,7\}$. Нехай $t = 1$. Тоді $x_1 = 8$, $x_3 = 8$. Окремим розв'язком рівняння (14) будуть числа $\{8,2,8\}$.

Для отримання цілочислових додатних значень "частоти" виникнення збитків x_j в розглядуваній моделі кількісного аналізу ризиків крім обмежень, які обумовлені методами розв'язання ЛДР при $n = 2$, необхідне також виконання додаткової умови $y_1 < q_2 x_2 - q_3 x_3$.

Метод 3.

Розглянемо рівняння (9). Нехай $a_1 > a_2$. Розділимо a_1 на a_2 з лишком і отримаємо: $a_1 = a_2 u + v$. Підставимо даний вираз в (9). Отримаємо $(a_2 u + v)x_1 + a_2 x_2 + a_3 x_3 = r$ або $a_2(ux_1 + x_2) + vx_1 + a_3 x_3 = r$.

Нехай $t_1 = ux_1 + x_2$. Тоді рівняння буде мати вигляд $3t_1 + x_1 + a_3 x_3 = r$. При $t_2 = a_3 x_3$ отримаємо: $3t_1 + x_1 + t_2 = r$. Отже: $x_1 = r - a_2 t_1 - t_2$, $x_2 = t_1 - x_1 = t_1 - (r - a_2 t_1 - t_2) = a_2 t_1 + t_1 + t_2 - r$, $x_3 = \frac{t_2}{a_3}$, де $t \in Z$.

Цілочислові додатні розв'язки рівняння (9) можна отримати при виконанні додаткової умови: $a_2 t_1 + t_1 + t_2 > r$ і t_2 буде без лишку ділитися на a_3.

Приклад. Розв'яжемо в цілих числах рівняння:

$$4x_1 + 3x_2 + 2x_3 = 54. \qquad (17)$$

Розділимо з лишком 4 на 3. Отримаємо $4 = 3(1) + 1$. Запишемо рівняння (17) в такому вигляді: $3(x_1 + x_2) + x_1 + 2x_3 = 54$. Після заміни $t_1 = x_1 + x_2$ рівняння буде мати такий вигляд: $3t_1 + x_1 + 2x_3 = 54$.

Нехай $t_2 = 2x_3$. Тоді $3t_1 + x_1 + t_2 = 54$. Після виконання перетворень отримаємо розв'язок рівняння (15) в такому вигляді: $x_1 = 54 - 3t_1 - t_2$, $x_2 = t_1 - x_1 = t_1 - (54 - 3t_1 - t_2) = 4t_1 + t_2 - 54$, $x_3 = \frac{t_2}{2}$, де $t \in Z$.

При розв'язанні рівняння (17) цілочислові додатні результати будуть отримані при виконанні додаткових умов: $3t_1 + t_2 < 54, 4t_1 + t_2 > 54$, а t_2 – парне додатне число, яке знаходиться в межах $54 - 4t_1 < t_2 < 54 - 3t_1$. Отже, при розв'язанні рівняння (17) для t_1 можуть бути задані умови: $\frac{54 - t_2}{4} < t_1 < \frac{54 - t_2}{3}$. Окремим розв'язком даного рівняння при $t_1 = 14$ і $t_2 = 2$ будуть числа $\{10, 3, 1\}$. Такі ж міркування можливіпри розв'язанні задачі пошуку "частоти" виникнення збитків в розглядуваній моделі ризику.

Якщо елементи рівняння (3) являють собою багаторозрядні числа, то для отримання його розв'язків можна скористатися результатами, які містяться, наприклад, у [10, 11].

Висновки

В роботі проведено аналіз відомих методів розв'язання лінійних діофантових рівнянь, які застосовуються в процесі моделювання ризиків. Отримані результати дозволяють накласти на досліджувану модель обмеження, які властиві області додатних цілих чисел, що, у свою чергу,дозволяє здійснити перехід від розгляду нескінченної множини розв'язків до розв'язку задачі перебору з допустимою кількістю розглядуваних варіантів.

Література

1. *ISO/IEC 31010:2009* Risk management – Risk assessment techniques.

2. *ISO/IEC 27001:2005* Information technology – Security techniques – Information security management systems – Requirements.

3. ЗайцевД.А. О реализации композиционных алгоритмов решения систем линейных уравнений / Д.А. Зайцев // Управляющие системы и машины. – 2006. – № 3. – С. 32-41.

4. Богоявленский Ю.А. Общий вид решения системы линейных диофантовых уравнений, ассоциированной с контекстно-свободной грамматикой / Ю.А. Богоявленский, Д.Ж. Корзун // Труды Петрозаводского государственного университета. Сер. “Прикладная математика и информатика”. Вып. 6. Петрозаводск: Изд-во ПетрГУ, 1998. – С.79-94.

5. Основы теории делимости чисел. Решение уравнений в целых числах. Факультативный курс/ [В.В. Бардушкин, И.Б. Кожухов, А.А. Прокофьев, Т.П. Фадеичева]. – М.: МГИЭТ(ТУ), 2003. – 224 с.

6. Схрейвер А. Теория линейного и целочисленного программирования: в 2-х т. Т. 1: пер с англ. – М.: Мир, 1991. –360с.

7. Безштанько В.М. Анализ результатов испытаний генетических алгоритмов при количественном расчетерисков информационной безопасности в условиях отсутствия статистических данных о частости реализации угроз/ В.М.Безштанько, С.И.Душкевич // Збірник наукових праць Інституту проблем моделювання в енергетиці НАН України. – К.: ІПМЕ, 2011. – Вип. 60. – С. 69-75.

8. Банникова Т.М. Основы теории чисел: учебно-методическое пособие /Т.М. Банникова, Н.А. Баранова. – Ижевск: Изд-во УдмуртГУ, 2009. – 95 с.

9. Азовская Т.В. Задачи по теории чисел: учебное пособие / Т.В. Азовская, В.В. Севастьянова. – Самара: Изд-во “Самарский университет”. – 2009. – 72 с.

10. Зінченко Я.В. Методи обчислення добутку багаторозрядних чисел та їх оптимізація. Частина І / Я.В. Зінченко // Сучасний захист інформації. – 2013. – № 4. – С. 39-47.

11. Зінченко Я.В. Методи обчислення добутку багаторозрядних чисел та їх оптимізація. Частина ІІ / Я.В. Зінченко // Сучасний захист інформації. – 2014. – № 3. – С. 45-53.

Надійшла 29.01.2015 р. Рецензент: д.т.н., проф. Барабаш О.В.