Висновки

Отриманий в результаті застосування розглянутої методики голосовий статистичний образ диктора є правдоподібним описом сигналу, який досліджується; образ є зручним для подальшого використання та зрозумілий для вивчення. Передбачена деталізація представлення голосового статистичного образу диктора. Мовний сигнал, який піддається процедурі обробки за пропонованою методикою, не підлягає усередненню. В цьому випадку втрат інформаційної повноти відображення характерних особливостей будови мовотворчого тракту диктора немає. Для вирішення завдання щодо ідентифікування джерела мовного сигналу усі сегменти аналізу мовної реалізації можуть бути задіяними. Суттєва асиметрія речовинного Хартлі спектру сигналу надає додаткові риси відмінності до голосових статистичних образів дикторів порівняно із комплексним спектром Фур'є сигналу, який досліджується.

*Література: **1**. Сапожков М. А. Речевой сигнал в кибернетике и связи – М.: Гос. изд-во л-ры по вопр. связи и радио, 1963.-с. 368 – 377. **2**. Рамишвили Г. С. Автоматическое опознавание говорящего по голосу / Москва, «Радио и связь», 1981. – 224 с. **3**. Новосельский А. Ф. Измерительный аппаратно – программный комплекс для идентификации личности по голосу: Дис. Канд.техн.наук: 05. 11. 16.-Киев, 1998. - 192 с. **4**. Женило В. Р. Минаев В. А. Компьютерные технологии в криминалистических фоноскопических исследованиях и экспертизах / Учебное пособие.-М.: Академия МВД РФ, 1994.– 137 с. **5.** Селетков В. Л. Соотношения связи одномерных преобразований Фурье и Хартли. // Радиоэлектроника, 2002.- № 7,- с. 46 – 50. (Изв. высш. учеб. заведений). **6.** Селетков В. Л. "Соответствие операций обработки сигналов при использовании преобразования Хартли" // Радиоэлектроника, 2002.– № 6 – с. 36 – 44. (Изв. высш. учебн. заведений). **7**. Селетков В .Л. "Модифицированное преобразование Хартли" // Радиоэлектроника, 1997.– № 1 – с. 75 – 77. (Изв. высш. учебн. заведений). **8**. Кузнецов М. В."Метод обработки речевых сигналов в системах спектральной идентификации" // Збірник наукових праць НА СБ України, 2006. – № 14. **9.** Шелухин О. И. Лукьянцев Н. Ф. Цифровая обработка и передача речи. / Под. ред. О. И. Шелухина.- М.: Радио и связь, 2000.- 456.: ил.- с. 98 – 106. **10.** Журавлев В. Н. "Анализ влияния частоты дискретизации на точность цифровой обработки речевых сигналов в системах биометрической идентификации" // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2005.– № 10 – с.51 – 59. **11.** Дейвуд Дж. Порядковые статистики: Пер. с англ. – М.: Мир, 1989.-540 с., ил.*

УДК 681.3.06

СИНТЕЗ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ, ОПТИМАЛЬНОЇ ЗА РІВНЕМ РИЗИКУ

Юрій Боня, Олексій Новіков

Фізико-технічний інститут Національного технічного університету України "КПІ"

Анотація: **Запропоновані алгоритми розв'язання задач математичного програмування, що виникають в процесі проектування відкритих систем захисту інформації, оптимальних за рівнем ризику. Використання методів сепарабельного та лінійного бульового програмування дозволило побудувати працездатні та ефективні алгоритми, що можуть використовуватися як складові спеціалізованих систем автоматизованого проектування систем захисту інформації.**

Summary: **Solution algorithms of mathematical programming tasks were proposed, which emerge during design of information protection systems with open architecture which provide optimal risk level. Use of separable and linear Boolean programming methods made it possible to develop algorithms capable of efficient working as a component of particularized computer aided design systems of information protection systems.**

Ключові слова: **Системи захисту інформації, ризик, загроза, відкриті системи, автоматизоване проектування, бульове програмування, сепарабельне програмування.**

І Вступ

Існують декілька концепцій побудови систем забезпечення мінімуму ризику (безпеки): "нульового ризику", "ненульового ризику" та змішаний підхід [1]. Концепція "нульового ризику" має іншу назву – детерміністський підхід при забезпеченні мінімуму ризику. В її основі лежить припущення, що можна виключити будь-яку небезпеку, якщо не пожалкувати грошей на побудову системи мінімізації ризику та забезпечити високий рівень дисципліни. Ця концепція є неадекватною щодо внутрішніх законів бізнесу,

функціонування банків та складних технічних систем. Згадані закони мають ймовірнісний характер і ризик завжди існує. Концепція "ненульового ризику" або концепція "прийнятного ризику" базується на чисельній оцінці ймовірності фінансової або технічної катастрофи. Ймовірнісний аналіз та керування ризиками дозволяє застосувати множину нових заходів для підвищення безпеки та зниження ризику, цілеспрямовано концентрувати та перерозподіляти засоби не лише для попередження фінансових або технічних катастроф, а і для завчасної підготовки до дій в екстремальних умовах. Під чисельним вимірюванням ризику розуміють або визначення ймовірності складної події, що ініціюється елементарними подіями, або обчислення середніх втрат (усереднення відбувається за допомогою обчислення суми всіх потенційних втрат з вагами, що пропорційні ймовірностям виникнення цих втрат). Після чисельного вимірювання ризику можливо встановити його припустимі норми. Відсутність методів чисельного вимірювання ризику призводить до того, що рішення, що приймаються для підвищення безпеки та зниження рівня ризику, є невизначеними за своїм характером.

Існує великий досвід розробки моделей ризику, безпеки та застосування логіко-ймовірнісного методу в атомній індустрії, морському флоті та ін. Такі системи є структурно складними та включають в себе обладнання, комп'ютерні та програмні засоби, дії персоналу з обслуговування, тестування та керування. Для багатьох сучасних систем ризик став нормальним явищем, бо їх функціонування за своєю природою пов'язано з виникненням ризику (такими є, наприклад, банківські системи, в яких завжди є ризик неповернення кредитів). Для того, щоб моделювати та оцінювати безпеку реального світу, необхідні різні моделі та потужні інформаційні технології. Поряд з застосуванням логіко-ймовірнісного методу для дослідження технічних систем існують та ефективно використовуються моделі банківських ризиків та шахрайства в бізнесі.

Інформація, що обробляється в сучасних інформаційно-телекомунікаційних системах (ІТС), завжди має певну цінність, хоча дуже часто її важко визначити кількісно. Нульовий ризик можна було б забезпечити, якби всі загрози інформації, що виникають в процесі її функціонування, ефективно нейтралізувалися засобами захисту, що були включені у відповідну систему захисту інформації (СЗІ). На практиці досягнення нульового рівня ризику не є реальним. Оскільки з міркувань здорового глузду вартість СЗІ не має перевищувати максимальні втрати від реалізації загроз, то звичайно вважається, що вартість СЗІ повинна становити не більше визначеного відсотку від втрат в найгіршому випадку.

Керування ризиками в ІТС має свої особливості, що описані в міжнародних стандартах в галузі захисту інформації [2, 3]. В згаданих стандартах було введено поняття про залишковий ризик, що є інтегральним показником, який відображає величину потенційних втрат, що можуть виникнути після успішної реалізації загроз інформації в певній СЗІ, і може розглядатися як один з критеріїв якості таких систем. При проектуванні такого класу структурно-складних технічних систем, як сучасні СЗІ, робота має вестися саме в напрямку мінімізації або обмеження величини ризику. В системах, що належать державним установам, на побудову СЗІ може виділятися певний бюджет, відповідно накладається обмеження на сукупну вартість використаних засобів захисту, а ймовірність порушення безпеки мінімізується. В системах, що експлуатуються в комерційних структурах, метою може бути побудова СЗІ з мінімальною вартістю при накладанні обмеження на величину ризику.

В [4] було запропоновано математичну модель, що описує ймовірність збереження захищеності інформації в ІТС з відкритою архітектурою. Також було сформульовано задачу математичного програмування, що виникає при синтезі СЗІ, що має мінімізувати ймовірність порушення безпеки за умови накладання обмеження на вартість засобів захисту, що входять до її складу. Задача математичного програмування мала вигляд

$$\begin{cases} \prod_{i=1}^{L}\left[1-\sum_{j=1}^{N}\left(E_{ij}\prod_{k=1}^{j-1}(1-E_{ik})\prod_{k=1}^{j}\left(1-\alpha_{ik}M_{ik}\right)\right)\right] \to \max\limits_{M_{ik}\in\{0,1\}}, \\ \sum_{i=1}^{L}\sum_{j=1}^{N}M_{ij}C_{ij} \le C_{\max}, \end{cases} \tag{1}$$

де N – кількість рівнів стеку протоколів ІТС; L – кількість загроз інформації та засобів захисту; E_{ik} – показник ефективності реалізації *i*-ї загрози інформації на *k*-му рівні; M_{ik} – параметр, значення якого (0 чи 1) визначає наявність *i*-го механізму захисту, реалізованого на *k*-му рівні; α_{ik} – коефіцієнт міцності *i*-го механізму захисту, реалізованого на *k*-му рівні.

Метою даного дослідження було обрано розробку алгоритмів розв'язання задачі (1), відмінних від градієнтних методів, та розгляд низки окремих випадків, що виникають при накладанні певних обмежень.

II Випадок з відсутністю дублювання засобів на різних рівнях

Оскільки для випадку абсолютно надійних засобів захисту їх реалізація має сенс лише на одному рівні стеку протоколів (неоптимальність конфігурацій, в яких засоби дублюються на кількох рівнях, доведена в [5]), то загальний вираз для цільової функції задачі (1) можна спростити. Також подібну конфігурацію СЗІ можна створити штучно. Хоч вона і не обов'язково буде оптимальною, але може виявитися прийнятною. В обох випадках для кожної i-ї загрози справджується $\sum_{j=1}^{N} M_{ij} \le 1$. Ця нерівність дозволяє стверджувати, що $\prod_{j=1}^{n}(1-\alpha_{ij}M_{ij}) = 1-\sum_{j=1}^{n}\alpha_{ij}M_{ij}$ (для абсолютно надійних засобів захисту $\alpha_{ij}=1$, а для загального випадку $0 \le \alpha_{ij} \le 1$). Тоді загальний вигляд задачі (1) спрощується, бо справджуються рівності

$$\prod_{i=1}^{L}\left[1-\sum_{j=1}^{N}\left(E_{ij}\prod_{k=1}^{j-1}(1-E_{ik})\prod_{k=1}^{j}(1-\alpha_{ik}M_{ik})\right)\right] =$$

$$= \prod_{i=1}^{L}\left[1-\sum_{j=1}^{N}\left(E_{ij}\prod_{k=1}^{j-1}(1-E_{ik})\right)+\sum_{j=1}^{N}\left(E_{ij}\sum_{k=1}^{j}\alpha_{ik}M_{ik}\prod_{k=1}^{j-1}(1-E_{ik})\right)\right],$$

$$\sum_{j=1}^{N}\left(E_{ij}\sum_{k=1}^{j}\alpha_{ik}M_{ik}\prod_{k=1}^{j-1}(1-E_{ik})\right) = \sum_{j=1}^{N}\alpha_{ij}M_{ij}\prod_{k=1}^{j-1}(1-E_{ik})(1-\prod_{k=j}^{N}(1-E_{ik})),$$

$$1-\sum_{j=1}^{N}E_{ij}\prod_{k=1}^{j-1}(1-E_{ik}) = \prod_{j=1}^{N}(1-E_{ij}).$$

Позначимо $A_{ij} = \alpha_{ij}\left(\prod_{k=1}^{j-1}(1-E_{ik}) - \prod_{j=1}^{N}(1-E_{ij})\right)$, $B_i = \prod_{j=1}^{N}(1-E_{ij})$, тоді в скороченому вигляді задача синтезу СЗІ, що забезпечує максимальну ймовірність збереження безпеки за умови накладання обмежень на вартість системи і відсутності дублювання засобів, буде мати наступний вигляд:

$$\begin{cases} \prod_{i=1}^{L}\left(B_i + \sum_{j=1}^{N}A_{ij}M_{ij}\right) \to \max\limits_{M_{ij}\in\{0,1\}}, \\ \sum_{i=1}^{N}M_{ij} \le 1,\ j=\overline{1,L},\ \sum_{i=1}^{L}\sum_{j=1}^{N}M_{ij}C_{ij} \le C_{\max}. \end{cases} \tag{2}$$

Отримана задача нелінійного бульового програмування може розв'язуватися як точними методами, так і наближеними. Для розв'язання задачі (2) наближеними методами, зокрема локально-стохастичними, запишемо її у вигляді задачі сепарабельного програмування. Такий запис також дозволить застосувати точний метод послідовного аналізу варіантів (ПАВ) [6, 7]. Отже, замість бульових змінних, що позначають, на якому рівні ми реалізовуємо механізм захисту, введемо цілі змінні, що набувають значень $0,\ldots,N$. Зв'язок буде наступним:

$$x_i = s-1,\ s=1,\ldots,N \Leftrightarrow M_{is}=1,$$
$$x_i = N \Leftrightarrow M_{is}=0 \quad \forall s=1,\ldots,N.$$

Задача (2) еквівалентна наступній:

$$\max_{x_i\in\{0,N\}}\left\{\sum_{i=1}^{L}F_i(x_i)\ \middle|\ \sum_{i=1}^{L}G_i(x_i) \le C_{\max}\right\},$$

де

$$\begin{cases} F_i(x_i) = \begin{cases} \sum_{k=1}^{x_i}\ln(1-E_{ik}),\ x_i=1,\ldots,N, \\ 0,\ x_i=0 \end{cases} \\ G_i(x_i) = \begin{cases} C_{ix_i},\ x_i=0,\ldots,N-1, \\ 0,\ x_i=N \end{cases} \end{cases}.$$

III Загальний випадок з неідеальними засобами захисту

Розглянемо загальний випадок, коли засоби захисту не є абсолютно надійними, і кожен засіб може реалізовуватися на всіх рівнях стеку, а не лише на одному, як було раніше. В [8] задача (1) розв'язувалася градієнтними методами. Після запису задачі (1) у вигляді задачі цілочисельного сепарабельного програмування для її розв'язання можуть використовуватися вже згаданий точний метод ПАВ, та методи локальної оптимізації (такі, як метод вектора спаду та локально-стохастичні алгоритми [9, 10]).

Оскільки задачі дискретного сепарабельного програмування припускають, щоб множини значень, які приймають змінні x_i, відрізнялися для різних i, то перейдемо до випадку, коли механізми захисту можуть реалізовуватися на кількох рівнях стеку, але не обов'язково на всіх N. Пропонується розв'язувати таку задачу за допомогою переходу до задачі цілочисельного сепарабельного програмування. Для цього необхідно зробити додаткові обчислення, що полягають у наступному. Нехай для кожної i-ї загрози існує набір номерів рівнів стеку $\{s_{i0},\ldots,s_{iv_i}\}$, $v_i < N$, на яких можна реалізувати відповідний механізм захисту. Тоді цілочисельна змінна x_i нової задачі буде приймати значення $0,\ldots,2^{v_i}-1$. В результаті нову задачу можна записати у вигляді

$$\min_{x_i\in\{0,2^{v_i}-1\}}\left\{\sum_{i=1}^{L}F_i(x_i)\,\middle|\,\sum_{i=1}^{L}G_i(x_i)\le C_{\max}\right\}, \tag{3}$$

де значення функцій $F_i(x_i)$ та $G_i(x_i)$ легко отримати, підставивши в i-й множник цільової функції та i-й доданок обмеження задачі (1) комбінацію бульових змінних, якій відповідає значення змінної x_i. Отриману задачу можна розв'язувати за допомогою методу ПАВ та наближених методів локальної оптимізації (методу вектора спаду та локально-стохастичних методів).

В загальному випадку, коли засоби захисту не є абсолютно надійними, та можуть реалізовуватися на всіх рівнях стеку, задача (3) може мати достатньо велику розмірність, бо кожна змінна x_i тоді може набувати 2^N-1 значень. На практиці багато з цих значень неможливо реалізувати, тому розмірність множини X_i є набагато меншою – не більше за $2^{N-s}-1$, де $s<N$ є кількістю заборонених рівнів, на яких даний засіб захисту не можна реалізувати. Для випадку, коли засіб може реалізовуватися не більш ніж на одному рівні, маємо $|X_i| = N+1$.

Вихідну задачу (1) також можна розв'язати за допомогою точного методу Балаша з модифікаціями Джеофріона [11], який припускає, щоб цільова функція задачі бульового програмування була нелінійною. Єдине, що вимагається – цільова функція повинна мати вигляд, що дає можливість однозначно знайти найкраще доповнення часткового розв'язку. Функція для нашого випадку очевидно є саме такою – для будь-якої бульової змінної значення 1 є кращим, ніж значення 0, якщо ми максимізуємо цю функцію. Нехай є частковий розв'язок $\widetilde{M}$, тоді для побудови найкращого доповнення $\widetilde{M}$ необхідно всім змінним, що не входять в $\widetilde{M}$, надати значення 1. Порушення обмеження на цьому етапі не враховується.

Замість бульової матриці з компонентами M_{ij}, $i=1,\ldots,L$, $j=1,\ldots,N$ будемо розглядати вектор з компонентами $x_{(i-1)N+j}=M_{ij}$. Позначимо через $\overline{Z}$ нижню границю значення цільової функції, відому на цей час (якщо на початку роботи ніякої інформації нема, то $\overline{Z}=0$). Будемо зберігати координати часткового розв'язку, що аналізується на поточному кроці алгоритму, у списку S. Точніше, будемо заносити в цей список число i, якщо $x_i=1$, та $-i$, якщо $x_i=0$. Змінні з індексами, які не включені до списку S (не важливо з яким саме знаком), вважаються вільними. Також в списку S кожний індекс може бути підкресленим, що вказує на те, що для цього часткового розв'язку зміна знаку індексу призведе до зменшення значення цільової функції на всіх можливих доповненнях, або до порушення нерівності. Для кожного часткового розв'язку, що відповідає поточному заповненню списку S, розглядається його найкраще доповнення x^S, координати якого для фіксованих змінних встановлюються відповідно до індексів із списку, а для вільних – так, щоб максимізувати цільову функцію не зважаючи на можливе порушення нерівності. Для нашої задачі для максимізації цільової функції всі вільні змінні потрібно встановити в одиницю.

Метод Балаша, адаптований для нашої задачі, буде мати наступний вигляд:

1. нехай $\overline{Z}$ – нижня границя значення цільової функції. Очистимо список S;
2. всі змінні x_i, які не є вільними, встановити згідно з заповненням S; всі вільні змінні x_i покласти рівними одиниці; зберегти цей розв'язок x^S; обчислити значення цільової функції на цьому розв'язку $f(x^S)$;
3. обчислити величину нев'язки $y^S = cx^s - C_0$; якщо $y^S \le 0$, то перейти до кроку 7;
4. додати до списку T^S ті вільні індекси j, які задовольняють умові $f(x^S \setminus x_j) > \overline{Z}$, де вектор $x^S \setminus x_j$ має ті самі координати, що і x^S, за винятком однієї координати $x_j = 0$;
5. обчислити величину $W = y^S - \sum_{j \in T^S} c_j$; перевіряємо, чи виконується $W > 0$; якщо це так, то поточний частковий розв'язок не можна доповнити таким чином, щоб не порушувалася нерівність, і переходимо до кроку 8, де буде зроблено перехід до іншого часткового розв'язку або відбудеться зупинка виконання алгоритму;
6. додати до списку S індекс $-j_0$, де $j_0 \in T^S$ і мінімізує величину $W_{j_0} = y^S - c_{j_0}$; повернутися до кроку 2;
7. якщо $f(x^S) > \overline{Z}$, то покласти $\overline{Z} = f(x^S)$, а розв'язок x^S зберегти як поточний найкращий;
8. знайти в списку S останній не підкреслений індекс; оскільки ми дійшли до цього кроку, то покращити розв'язок не можна, тому треба змінити знак індексу на протилежний і підкреслити, щоб вказати, що цей розв'язок вже прозондовано. Всі індекси після підкресленого треба знищити, бо щодо них ніяких висновків зробити не можна; якщо такого індексу не знайдено, то зупинитися і видати останній найкращий розв'язок з відповідним значенням $\overline{Z}$, інакше повернутися до кроку 2.

Для розв'язання задачі з реалізацією засобу захисту на єдиному рівні за допомогою методу Балаша також можливо вказати, як знаходити найкраще доповнення часткового розв'язку. Нехай є частковий розв'язок $\widetilde{M}$. Відомо, що він не порушує жодну нерівність, зокрема обмеження на структуру розв'язку. Для того, щоб знайти найкраще доповнення $\widetilde{M}$ для всіх $i = 1, \ldots, L$ необхідно зробити наступне. Якщо всі змінні $M_{ij} = 0$, $M_{ij} \in \widetilde{M}$, $j = 1, \ldots, N$, причому залишається хоча б одна вільна змінна M_{iq}, то покладаємо $M_{iq} = 1$, де q є мінімальним серед усіх вільних змінних для цього i. Якщо ж серед змінних $M_{ij} \in \widetilde{M}$, $j = 1, \ldots, N$ є одиниця, то, виходячи з необхідності виконання обмеження на структуру розв'язку, ми маємо покласти $M_{iq} = 0$, $q = 1, \ldots, N$ для всіх вільних змінних для цього i. Отриманий розв'язок і буде найкращим доповненням $\widetilde{M}$ (серед обмежень враховано лише обмеження на структуру розв'язку, а вартість системи на цьому етапі не розглядається).

IV Інші окремі випадки задачі

Розглянемо окремі часткові випадки загальної задачі (1), що використовувалися при дослідженні градієнтного методу [8], та можуть розв'язуватися більш ефективно з використанням еквівалентних переходів за допомогою відомих алгоритмів математичного програмування.

Розглянемо випадок, коли для кожної i-ї загрози існує єдиний рівень стеку s_i, на якому можна реалізувати механізм захисту, а для всіх інших рівнів вартість не визначалася (можна вважати її нескінченною). Показник ефективності реалізації i-ї загрози покладаємо ненульовим тільки для s_i-го рівня (того самого, на якому можливо реалізувати механізм захисту). Отриману нелінійну задачу (1) з LN бульовими змінними можна розв'язувати за допомогою різних методів, наприклад, градієнтного методу [8], модифікованого методу Балаша, подібного до викладеного вище, та за допомогою методів сепарабельного програмування. Для того, щоб відобразити забороненість деяких комбінацій змінних, в методі Балаша достатньо будувати часткові розв'язки, починаючи з такого, в якому відповідні змінні будуть зафіксовані (в термінах алгоритму це означає включення до списку S підкреслених індексів). В

інших методах також принципово можна врахувати обмеження на можливість реалізації засобів захисту, але простіше за все в згаданому випадку привести задачу до еквівалентної задачі лінійного бульового програмування (ЛБП). Отже, якщо в термінах задачі (1) маємо

$$E_{ij} = \begin{cases} e_i,\ j = s_i \\ 0,\ j \neq s_i \end{cases},\quad C_{ij} = \begin{cases} c_i,\ j = s_i \\ \infty,\ j \neq s_i \end{cases},\ \alpha_{ij} = 1,\quad i = \overline{1, L},\quad j = \overline{1, N},$$

то для кожної i-ї загрози існує дві можливості – використати механізм захисту, або відмовитися від протидії цій загрозі. В першому випадку ймовірність того, що загроза не зможе реалізуватися, дорівнює $1-(1-\alpha_{is_i})e_i$, а в другому – $1-e_i$. Після логарифмування залежність ймовірності протидії i-й загрозі буде наступною:

$$\log P_i = (1-x_i)\ln(1-e_i) + x_i \ln\left(1-(1-\alpha_{is_i})e_i\right) =$$
$$= \ln(1-e_i) + x_i \ln\left(\left(1-(1-\alpha_{is_i})e_i\right)/(1-e_i)\right),$$

де бульова змінна x_i позначає початкову змінну M_{is_i}.

Для визначення конфігурації оптимальної СЗІ достатньо розв'язати наступну задачу ЛБП:

$$\max_{x_i \in \{0,\,1\}} \left\{ \sum_{i=1}^{L} x_i \ln\left(\left(1-(1-\alpha_{is_i})e_i\right)/(1-e_i)\right) \middle| \sum_{i=1}^{L} c_i x_i \le C_0 \right\}. \tag{4}$$

Подібною також буде ситуація, коли механізми можна реалізувати на всіх рівнях, але кожна i-та загроза має ненульову ефективність реалізації лише на одному рівні стеку протоколів (позначимо його номер s_i). В цьому випадку знову достатньо розв'язати задачу ЛБП, наведену вище.

V Результати чисельних експериментів

Для перевірки працездатності розроблених алгоритмів та доведення коректності еквівалентних задач було проведено ряд чисельних експериментів. В п'ятьох випадках це були ті самі модельні приклади, що використовувалися для дослідження алгоритмів, описаних в [4, 8], і ще один був згенерований додатково. Для всіх прикладів засоби захисту вважалися абсолютно надійними.

Як перший приклад розглядалася СЗІ, ефективність реалізації всіх загроз в якій була однаковою і дорівнювала 0.05, причому ненульовою вона була тільки для одного рівня стеку протоколів для кожної загрози. Щодо матриці вартостей, то її елементи для *i*-го засобу захисту визначалися тільки для одного рівня стеку – того, на якому можна реалізувати цей засіб. Кількість загроз та механізмів захисту $L = 20$, а кількість рівнів стеку $N = 7$. Максимальна вартість засобів захисту, що входять до складу СЗІ, не мала перевищувати величини $C_{\max}$, що складала 50% від сумарної вартості всіх засобів захисту. Для знаходження оптимальної конфігурації СЗІ в цьому випадку достатньо було розв'язати задачу ЛБП вигляду (4). Для її розв'язання використовувалися алгоритм Балаша та метод вектора спаду, реалізовані у вигляді процедур бібліотеки чисельного аналізу НДОЦ МДУ [12] (процедури MNR3R та MLC6R). Про результати експериментів можна сказати наступне. Точний метод Балаша знайшов той самий глобальний максимум, що і градієнтний метод з [5], натомість метод вектора спаду знайшов тільки локальний. Відносна похибка отриманого локального максимуму склала 5% (0.6983 замість точного значення 0.7351). Початкова ймовірність збереження безпеки при повній відмові від реалізації засобів захисту склала $(1\text{-}0.05)^L = 0.3585$.

Як другий та третій приклад розглядалася СЗІ, ефективності реалізації загроз в якій відрізнялися, причому знову ненульовими вони були тільки для одного рівня стеку протоколів для кожної загрози. Відрізнялися приклади величиною максимальної вартості СЗІ, відповідно 50% та 93.4% від сумарної вартості всіх засобів захисту. Застосування згаданих алгоритмів розв'язання задачі ЛБП дозволило в обох випадках знайти той самий максимум (локальний співпав з глобальним), що був знайдений в [8] за допомогою градієнтного методу. В порівнянні з початковою ймовірністю збереження безпеки при повній відмові від реалізації засобів захисту $P_0 = \Pi(1\text{-}e_i) = 0.3547$ знайдені конфігурації СЗІ дозволили підвищити ймовірність відповідно до значень $P_1 = 0.9136$ та $P_2 = 0.9978$.

Як четвертий приклад розглядалася СЗІ, в якій кожна загроза мала ненульові ймовірності реалізації на трьох рівнях стеку протоколів з наявних $N = 7$, а на всіх інших рівнях засоби не могли реалізовуватися взагалі. Кількість загроз та засобів захисту L знову складала 20. Вартість реалізації засобів захисту була обернено пропорційною номеру рівня стеку. Обмеження вартості встановлювалося на рівень 19% від вартості конфігурації, в якій для кожної загрози механізм захисту реалізовувався на найнижчому

можливому рівні. Оптимальна конфігурація СЗІ знаходилася розв'язанням задачі сепарабельного програмування за допомогою локально-стохастичного алгоритму [10]. Порівняно з розв'язком, знайденим у [8], після повторного запуску алгоритму з різних початкових точок було знайдено конфігурацію СЗІ, що забезпечує приблизно еквівалентний рівень захисту – ймовірність складала $P' = 0.9516$ на відміну від значення $P = 0.9598$, знайденого градієнтного методу.

Як п'ятий приклад розглядалася СЗІ, в якій кожна загроза мала ненульові ймовірності реалізації на трьох рівнях стеку протоколів з наявних $N = 7$, але реалізовуватися засоби могли на будь-якому рівні. За допомогою кількаразового запуску локально-стохастичного алгоритму з різних початкових точок вдалося покращити розв'язок, знайдений за допомогою градієнтного методу. Отримане значення ймовірності збереження безпеки $P' = 0.947$ виявилося кращим за знайдене раніше $P = 0.901$.

Ймовірнісні характеристики загроз для шостого прикладу було згенеровано випадковим чином, вартість засобів була обернено пропорційною номеру рівня стеку. Стек протоколів містив $N = 4$ рівні, а кількість загроз та засобів захисту L складала 20.

Характер зміни ймовірності збереження захищеності при розв'язанні задач 4-6 в процесі роботи локально-стохастичного алгоритму можна прослідкувати на рисунку.

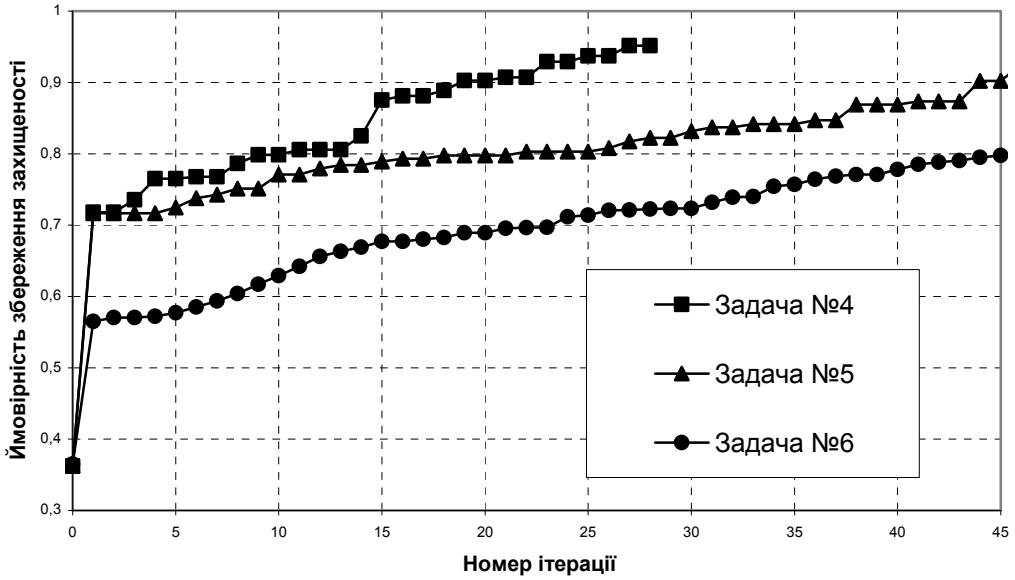

Рисунок – Збіжність алгоритмів при розв'язанні задач 4 – 6

VI Висновки

В роботі запропоновані алгоритми розв'язання задач математичного програмування, що виникають в процесі синтезу СЗІ в ІТС з відкритою архітектурою, які забезпечують максимальну ймовірність збереження безпеки. Розглянуто низку окремих випадків, в яких задача суттєво спрощується. Проведені експерименти свідчать про те, що викладені алгоритми є працездатними, ефективними та можуть використовуватися як складова спеціалізованих систем автоматизованого проектування СЗІ.

Література: ***1.*** *Соложенцев Е. Д., Соложенцев В. Е. Концепции обеспечения безопасности сложных систем: "нулевого риска", "ненулевого риска", смешанного подхода / Под ред. И. А. Рябинина, Е. Д. Соложенцева.– СПб.: ИПМАШ РАН, 1994. – Препринт 110. – Вып.4. – С. 67 – 82..* ***2.*** *ISO/IEC 17799, Information technology - Security techniques - Code of practice for information security management.* ***3.*** *ISO/IEC 2nd WD 13335-3, Information technology - Security techniques - Guidelines for the management of information and communications technology security - Part 3: Techniques for information and communications technology security risk management.* ***4.*** *Новіков А., Тимошенко А. Построение логико-вероятностной модели защищенной компьютерной системы // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.– 2001.– вип. 3.– С.101-105.* ***5.*** *Боня Ю. Ю., Новиков А. Н. Синтез систем защиты информации с минимальной стоимостью механизмов защиты // Проблемы управления и информатики.– 2006.– №3.– С.147-156.* ***6.*** *Михалевич В. С., Волкович В. Л. Вычислительные методы исследования и проектирования*

сложных систем.– М.: Наука, 1982.– 286 с. ***7.*** *Зайченко Ю. П. Исследование операций: 6-е изд.– К.: Слово, 2003.– 688 с.* ***8.*** *Новиков А., Тимошенко А. Определение множества механизмов защиты, обеспечивающих оптимальный уровень защищенности информации // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.– 2002.– вип. 4.– С.98 – 105.* ***9.*** *Сергиенко И. В. Математические модели и методы решения задач дискретной оптимизации.– К.: Наукова думка.– 1985. – 384 с.* ***10.*** *Сергиенко И. В., Лебедева Т. Т., Рощин В. А. Приближенные методы решения дискретных задач оптимизации.– К.: Наукова думка.– 1980. – 276 с.* ***11.*** *Geoffrion Arthur M. Integer Programming by Implicit Enumeration and Balas' Method // SIAM Review.– 1967.– Vol. 9, No. 2.– p. 178 – 190.* ***12.*** *Систематический каталог библиотеки численного анализа НИВЦ МГУ http://srcc.msu.su/num_anal/lib_na/cat/cat0.htm*

УД УДК 681.321;322:621.395

ФОРМУВАННЯ ВИМОГ ЩОДО БЕЗПЕКИ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ ЗАГАЛЬНОГО КОРИСТУВАННЯ

Сергій Гладиш
Одеська національна академія зв'язку ім. О. С. Попова

Анотація: **Досліджується проблема проектування системи інформаційної безпеки в телекомунікаційній мережі загального користування, в якій обробляються і передаються державні інформаційні ресурси з різним режимом доступу та різними вимогами безпеки. Проведено аналіз вітчизняних та міжнародних нормативних документів. Визначена ієрархія понять щодо державних інформаційних ресурсів та їхньої безпеки. Розроблено вимоги до системи інформаційної безпеки.**
Summary: **The problem of information security system projecting in public telecommunication network, in which state information resources with different access mode and different security requirements are processed and transmitted, is researched. Ukrainian and international normative documents are analyzed. The hierarchy of terms concerning to state information resources and their security is defined. The requirements of information security system are developed.**
Ключові слова: **Державні інформаційні ресурси, інформаційна безпека, телекомунікаційні мережі.**

І Вступ

Загальна проблема забезпечення інформаційної безпеки (ІБ) в телекомунікаційних мережах загального користування (ТМЗК) в останній час стає все більш важливою. Така тенденція зумовлена рядом чинників, головними з яких можна назвати наступні:

– динаміка розвитку та широке розповсюдження інформаційно-комунікаційних технологій як у державному секторі (національна система конфіденційного зв'язку, електронний уряд, інфраструктура центрів сертифікації ключів та електронного цифрового підпису, електронне голосування, телемедицина, дистанційне навчання), так і в недержавному (стаціонарні та мобільні мережі зв'язку загального користування, Інтернет, електронна комерція, приватні та відомчі корпоративні мережі тощо);

– високі вимоги до показників якості, сталості та безпеки телекомунікаційних мереж (ТМ) як базової складової сучасних інформаційно-телекомунікаційних систем (ІТС);

– висока критичність ТМЗК як основного технічного ресурсу національного інформаційного простору держави та як складової глобальної інформаційної інфраструктури.

В умовах переходу до інформаційного суспільства, поширення міжнародного тероризму, розвитку концепції інформаційної війни та розробки інформаційної зброї підвищується значущість ІБ як важливого компонента безпеки суспільства. ІБ держави є невід'ємною складовою частиною національної безпеки України. На відміну від США, де з 1963 р. існує автономна і фізично відокремлена від ТМЗК Національна система зв'язку (NCS) спеціального призначення [1], в Україні вся національна інформаційна інфраструктура, включаючи національну систему конфіденційного зв'язку та інші мережі спеціального призначення, принаймні на нижчих рівнях (фізичному, канальному) використовують канали магістральної первинної мережі ТМЗК (ВАТ «Укртелеком»). Це зумовлює актуальність завдання забезпечення ІБ державних інформаційних ресурсів в ТМЗК України.

Питанням створення комплексних систем захисту інформації (КСЗІ) в автоматизованих (інформаційних) системах (АС, ІС) присвячено багато робіт. На сьогодні в світі існує досить розвинута нормативна база щодо різних аспектів та етапів створення КСЗІ. На пострадянському просторі першим фундаментальним дослідженням, в якому була чітко сформульована методологія проектування КСЗІ є