До специфічних методів можна зарахувати метод “гібридного”, або часткового резервування. Цей метод передбачає захист як методом “дзеркало”, так і “перехресним” методом. У разі необхідності (важливості ділянки або слабких каналів зв’язку) використовується метод “дзеркало”, а в інших випадках – метод “перехресного” резервування.

Окремо можна відзначити можливість використання Web-сервісів для побудови динамічно кластерної нейронної мережі, що дають змогу легко, та не відходячи від об’єктної моделі, організовувати різноманітні конфігурації нейронної мережі. Також Web-сервіси дають можливість зберігати створений код за зміни структури мережі. Потрібно буде лише змінити відповідні файли налаштування.

*1. Жуков І.А., Кременецький Г.М. Динамічна просторово-логічна кластеризація нейронної мережі / Інформаційні технології та комп’ютерна інженерія. – Вінниця: ВНТУ, 2009. – Вип. 1(14). – С.39–43.*
*2. Кременецький Г.М., Журавель С.В. Гравітаційний метод динамічної кластеризації нейронної мережі / Проблеми інформатизації та управління: зб. наук. пр. – К.: НАУ, 2009. – Вип. 1(25). – С.86–89.*
*3. Кременецький Г.М. Побудова динамічної кластерної нейронної мережі з використанням WEB-сервісів / Проблеми інформатизації та управління: зб. наук. пр. – К.: НАУ, 2009. – Вип. 2(26). – С.76–81.*

**УДК 004.056**

**С.М. Кущ, В.О. Шутовський**
Національний технічний університет України “Київський політехнічний інститут”

# ПОБУДОВА КСЗІ НА ОСНОВІ РЕЗУЛЬТАТІВ ОЦІНКИ РИЗИКІВ ІБ МЕТОДОМ АНАЛІЗУ ГРАФА АТАК



**Запропоновано методику побудови КСЗІ ІС на основі результатів оцінки ризиків ІБ методом аналізу графа атак. Здійснено програмну реалізацію цієї методики. Наведено результати обчислювальних експериментів.**

**Ключові слова: інформаційна безпека, оцінка ризиків, комплексні системи захисту інформації, граф атак**

**The technique of complex information security systems construction is proposed. The technique is based on the results of information security risks assessment using an attack graph. A software solution for the technique was made and computational experiments were carried out.**

**Key words: information security, risks assessment, complex information security systems, attack graph**

## Вступ

Сучасна парадигма інформаційної безпеки (ІБ) приймає ризик-орієнтований підхід як стандартний підхід під час розроблення комплексних систем захисту інформації (КСЗІ) [1, 2], що уможливлює провести обґрунтоване конфігурування системи захисту інформаційної системи (ІС).

**Мета роботи –** побудувати КСЗІ ІС на основі результатів оцінки ризиків ІБ системи, отриманих методом аналізу графа атак.

## Оцінка ризиків ІБ ІС методом аналізу графа атак з нечіткими ваговими коефіцієнтами

Для оцінки ризиків ІБ ІС сьогодні запропоновано велику кількість методик. Ці методики можна розділити на якісні, напівкількісні та кількісні. Особливий інтерес являють собою кількісні

методики оцінки ризиків ІБ, які уможливлюють автоматизацію побудови КСЗІ ІС. Використання методу кількісної оцінки ризиків ІБ на основі аналізу графа атак [3] дає змогу провести автоматизацію як на першому етапі, так і в динаміці процесу оцінки ризиків ІБ ІС. Такий підхід враховує структуру ІС під час проведення оцінки ризиків ІБ і моделювання сценаріїв розгортання атак за різних конфігурацій КСЗІ.

Граф атак – це орієнтований граф $D = (V,E)$, який являє собою сукупність сценаріїв (трас атак), що моделюють нанесення збитків зловмисним агентом інформаційній системі, яка підлягає захисту. Метод оцінки ризиків ІБ ІС на основі аналізу графа атак використовується для аналізу захищеності комп'ютерних мереж, однак автори також запропонували використовувати його для аналізу систем різних типів [3]. Застосовуючи метод аналізу графа атак для оцінки ризиків ІБ ІС, зловмисник представляється групою агентів, які прагнуть порушити функціонування інформаційної системи. Метою сторони, що захищається, є зменшення збитків від реалізації ймовірних загроз.

У детермінованій моделі графа атак ваговий коефіцієнт дуги $e_{i,j} = \{u_i,u_j\}$ між довільними вершинами $u_i$ та $u_j$ дорівнює одиниці ($w_{i,j} = 1$): дуга моделює можливість переходу зловмисного агента до підсистеми $u_j$, якщо він знаходиться у підсистемі $u_i$. На основі детермінованої моделі графа атак запропоновано недетерміновану модель: ваговим коефіцієнтам графа атак присвоюються значення ймовірності переходу агента з однієї підсистеми до іншої [3].

У роботі проведено модифікацію моделі графа атак. Вузлами графа атак є: а) ініціюючі події; б) підсистеми, яким може бути завдано збитків; дугами графа атак $e_{i,j} = \{u_i,u_j\}$ – оцінки ризику переходу агента до підсистеми $u_j$, якщо до цього він знаходився у підсистемі $u_i$. Вагові коефіцієнти дуг графа атак $w_{i,j}$ обчислювалися на основі теорії нечітких множин.

Такий підхід дає змогу в процесі оцінювання ризиків ІБ оперувати вхідними даними різної форми (кількісними, напівкількісними та якісними) і проводити оцінювання ризиків ІБ для вхідних даних різної природи та отриманих з різних джерел.

**Побудова КСЗІ ІС на основі розрахованих оцінок ризиків ІБ**

Використання методу аналізу графа атак дадо змогу отримати детальну оцінку ризиків ІБ з урахуванням структури ІС та можливостей зловмисника використовувати різні вразливості системи. У результаті застосування методу для тестової системи отримано перелік ранжованих оцінок ризиків ІБ.

Для зменшення ризиків ІБ ІС до заданого рівня слід модифікувати КСЗІ. Наявність кількісних оцінок ризиків ІБ дає можливість застосувати набір формалізованих методів для розв'язання задачі побудови КСЗІ, причому у першому наближенні доцільно використовувати апарат лінійного програмування.

Кількісні оцінки ризиків ІБ ІС, отримані методом графа атак, є сумою вагових коефіцієнтів (оцінок ризиків ІБ) окремих дуг графа атак. Введення елементів системи захисту інформації (ЗІ) дає змогу зменшити значення вагового коефіцієнта (ризику ІБ) дуги графа атак. Засіб захисту інформації (ЗЗІ), окрім місця встановлення, характеризується коефіцієнтом ефективності (відношенням вартості ЗЗІ до величини зменшення ризику ІБ). Загалом між величиною зменшення ризику ІБ та вартістю засобів захисту інформації існує багатофакторна залежність. Однак у першому наближенні можна вважати, що між величиною зменшення ризику ІБ та вартістю ЗЗІ є лінійний зв'язок (тобто розрахунки проводяться на лінійній ділянці залежності величини зменшення ризику ІБ від вартості ЗЗІ [4]).

**Мета роботи –** визначити набір засобів захисту інформації, який забезпечить рівень ризику ІБ, менший від заданого, і при цьому матиме найменшу можливу вартість.

Ефективним методом обчислення такого набору ЗЗІ є лінійне програмування [5]. Система нерівностей, яка описує задачу зменшення рівня ризику ІБ ІС до порогового за мінімізації витрат, має такий вигляд:

$$
\begin{aligned}
&c_{11}x_{11} + c_{12}x_{12} + \ldots + c_{1k}x_{1k} + c_{21}x_{21} + \ldots + c_{n(k-1)}x_{n(k-1)} + c_{nk}x_{nk} \to \min;\\
&x_{11} + x_{12} + \ldots + x_{1k} \geq b_1;\\
&x_{21} + x_{22} + \ldots + x_{2k} \geq b_2;\\
&\ldots\\
&x_{n1} + x_{n2} + \ldots + x_{nk} \geq b_n;\\
&x_{ij} \geq 0 \forall i = 1,2,\ldots n;\ j = 1,2,\ldots k,
\end{aligned}
\qquad (1)
$$

де $c_{ij}$ – коефіцієнти ефективності засобів захисту; $x_{ij}$ – величини зменшення ризиків для кожної дуги графа атак; $b_i$ – величини, на які треба зменшити ризики.

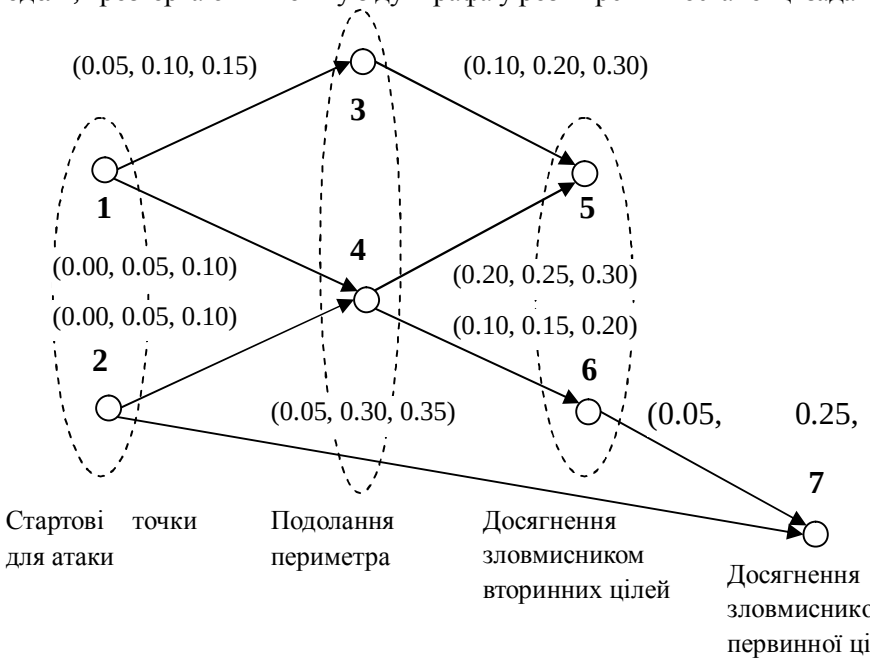
Кількість змінних у системі нерівностей дорівнює кількості складових ризиків ІБ, величина яких перевищує порогове значення ризику ІБ. Величина цього набору змінних не може перевищувати кількості дуг у графі атак ІС. Розв'язання задач лінійного програмування здійснюється переведенням системи нерівностей у стандартну форму і застосуванням симплекс-методу [5]. Задача розв'язується за кінцевий час, хоча алгоритм розв'язку не належить до поліноміальних.

Для розв'язання поставленої задачі було застосоване програмне забезпечення (ПЗ) для розв'язання задач змішаного цілочислового лінійного програмування з відкритим вихідним кодом lp_solve [6]. Було додатково розроблено програмний модуль для обчислення ризиків ІБ ІС, що перевищують задане порогове значення, що здійснює дефазифікацію значень ризиків ІБ та формує файл у форматі MPS [6], який подається на вхід програми lp_solve. Результати роботи програми lp_solve записуються у файл.

**Приклад побудови КСЗІ для ІС**

Для ілюстрації використання методу розглянуто застосування графа атак з нечіткими ваговими коефіцієнтами для оцінки ризиків ІБ тестової ІС, для якої побудовано граф атак, який складається з семи вершин і восьми дуг (рисунок). Вагові коефіцієнти розраховано з використанням нечіткої експертної системи на основі нормованих значень ймовірностей реалізації загроз та збитків від реалізації загроз [7].

На рисунку нечіткі вагові коефіцієнти графа атак подано трьома числами, що являють собою трикутне нечітке число вигляду ($a_1$, $a_M$, $a_2$), визначене на інтервалі [$a_1$, $a_2$] (тобто його функція належності у цих точках і за межами цього інтервалу дорівнює нулю), а в точці $a_M$ його функція належності приймає значення, що дорівнює 1 [8]. На основі отриманого графа атак можна побудувати деталізованішу модель, "розгортаючи" кожну з дуг графа у розширеній постановці задачі.




*Граф атак з нечіткими ваговими коефіцієнтами, побудований для тестової ІС*

На основі сформованого графа атак проведено оцінку ризиків ІБ ІС з використанням розробленого ПЗ. Ранжовані оцінки ризиків ІБ ІС, середнє значення яких перевищує задане порогове значення 0.25, наведено у табл. 1.

*Таблиця 1*

**Ранжовані оцінки ризиків ІБ тестової ІС**

| № | Шлях | Сумарний ризик |
|---|---|---|
| 1 | 1->4->6->7 | (0.15, 0.45, 0.60) |
| 2 | 2->4->6->7 | (0.15, 0.45, 0.60) |
| 3 | 1->3->5 | (0.15, 0.30, 0.45) |
| 4 | 1->4->5 | (0.20, 0.30, 0.40) |
| 5 | 1->4->5 | (0.20, 0.30, 0.40) |
| 6 | 2->7 | (0.05, 0.30, 0.35) |

На основі ранжованих оцінок ризиків ІБ, одержаних в результаті розрахунків розробленим ПЗ, для побудови КСЗІ був сформований файл (у форматі mps), і здійснено розв'язання задачі лінійного програмування з чіткими коефіцієнтами нерівностей. Відповідність дуг графа атак змінним задачі лінійного програмування наведено у табл. 2.

*Таблиця 2*

**Відповідність дуг графа атак змінним у задачі лінійного програмування**

| № | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Дуга | 1->3 | 1->4 | 2->4 | 2->7 | 3->5 | 4->5 | 4->6 | 6->7 |
| Змінна | $x_0$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $x_6$ | $x_7$ |

Для спрощення аналізу на цьому етапі розв'язання коефіцієнти ефективності контрзаходів для будь-якої дуги графа атак були прийняті однаковими. У цьому випадку система нерівностей набуває такого вигляду:

$$\begin{aligned}
&x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 \to \min;\\
&x_1 + x_6 + x_7 \geq 20;\\
&x_2 + x_6 + x_7 \geq 20;\\
&x_6 + x_7 \geq 15;\\
&x_0 + x_4 \geq 5;\\
&x_2 + x_5 \geq 5;\\
&x_3 \geq 5;\\
&x_i \geq 0 \forall i = 1,2,...7.
\end{aligned} \qquad (2)$$

Розв'язок задачі був проведений утилітою розв'язання задач змішаного цілочислового лінійного програмування з відкритим вихідним кодом lp_solve. Результати розрахунків наведено у табл. 3. Необхідне зменшення ризику у табл. 3 розраховане з використанням ПЗ для забезпечення рівня ризику ІБ, меншого від заданого. Час роботи $t$ для задачі такої розмірності на ПК (для ноутбука Acer 3810T, процесор Intel Core 2 Solo, частота – 1.4 ГГц, розмір ОЗУ – 4 Гб) становить менше однієї секунди ($t < 1$ *с*). Розв'язання задачі для 65 змінних та 135 нерівностей займає близько однієї секунди ($t \approx 1$ *с*).

*Таблиця 3*

**Результати розв'язання задачі побудови КСЗІ для тестової ІС**

| № | Дуга | Змінна | Необхідне зменшення ризику |
|---|---|---|---|
| 1 | 1->3 | $x_0$ | 5 |
| 2 | 1->4 | $x_1$ | 5 |
| 3 | 2->4 | $x_2$ | 5 |
| 4 | 2->7 | $x_3$ | 5 |
| 5 | 3->5 | $x_4$ | 0 |
| 6 | 4->5 | $x_5$ | 0 |
| 7 | 4->6 | $x_6$ | 15 |
| 8 | 6->7 | $x_7$ | 0 |

Практичний інтерес являє собою розв'язання задачі для випадку різних коефіцієнтів ефективності ЗЗІ для ансамблю дуг графа атак. Оцінки коефіцієнтів ефективності засобів захисту для різних дуг графа атак отримано з бази знань ЗЗІ і наведено у табл. 4.

*Таблиця 4*

**Оцінки коефіцієнтів ефективності засобів захисту для дуг графа атак**

| № | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Дуга | 1->3 | 1->4 | 2->4 | 2->7 | 3->5 | 4->5 | 4->6 | 6->7 |
| Змінна | $x_0$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $x_6$ | $x_7$ |
| Коефіцієнт ефективності | 0.5 | 0.4 | 0.4 | 0.8 | 0.2 | 0.5 | 0.8 | 0.6 |

Для цього випадку система нерівностей набуває такого вигляду:

$$
\begin{aligned}
&0.5x_0 + 0.4x_1 + 0.4x_2 + 0.8x_3 + 0.2x_4 + 0.6x_5 + 0.5x_6 + 0.8x_7 \to \min;\\
&x_1 + x_6 + x_7 \geq 20;\\
&x_2 + x_6 + x_7 \geq 20;\\
&x_6 + x_7 \geq 15;\\
&x_0 + x_4 \geq 5;\\
&x_2 + x_5 \geq 5;\\
&x_3 \geq 5;\\
&x_i \geq 0 \forall i = 1,2,...7.
\end{aligned}
\qquad (3)
$$

Результати розв'язання задачі наведено у табл. 5.

*Таблиця 5*

**Результати розв'язання задачі побудови КСЗІ для тестової ІС для різних коефіцієнтів ефективності засобів захисту інформації**

| № | Дуга | Змінна | Розраховане зменшення ризику |
|---|---|---|---|
| 1 | 1->3 | $x_0$ | 0 |
| 2 | 1->4 | $x_1$ | 5 |
| 3 | 2->4 | $x_2$ | 5 |
| 4 | 2->7 | $x_3$ | 5 |
| 5 | 3->5 | $x_4$ | 5 |
| 6 | 4->5 | $x_5$ | 0 |
| 7 | 4->6 | $x_6$ | 0 |
| 8 | 6->7 | $x_7$ | 15 |

Порівнюючи результати розв'язання задачі за двох наборів коефіцієнтів ефективності засобів захисту ІС, наведених у табл. 3 і 5, можна зробити висновок, що для одержання оптимального варіанта системи захисту інформації, необхідно проводити розрахунки за різних сценаріїв.

**Висновки**

Результати проведеного дослідження дають підстави зробити такі висновки:

1. Використання розробленої методики дає змогу здійснити побудову КСЗІ інформаційної системи на основі розв'язку задачі лінійного програмування, застосовуючи методику оцінки ризиків ІБ на основі аналізу графа атак з нечіткими ваговими коефіцієнтами.

2. Методика, запропонована у роботі, уможливлює мінімізувати вартість КСЗІ ІС під час забезпечення значень ранжованих ризиків ІБ ІС, що не перевищують задане значення. Застосування запропонованого способу можливе не тільки за побудови КСЗІ "з нуля", але і за модифікації вже існуючої КСЗІ. Програмна реалізація не є ресурсовитратною, час її роботи на ПК дає можливість отримати розв'язок за прийнятний час.

3. Перспективним напрямом подальших досліджень побудови КСЗІ ІС є розв'язання задач нелінійного та дискретного програмування на основі результатів оцінки ризиків ІБ методом аналізу графа атак.

*1. Information technology – Security techniques – Information security management systems – Requirements: ISO/IEC 27001:2005. – [Чинний від 15-10-2005]. – Женева: [б.в.], 2005. – 42 с. – (Міжнародні стандарти ISO/IEC). 2. Gary Stoneburner. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology: NIST SP 800-30. – [Електронний ресурс] // NIST.gov. – Computer Security Division – Computer Security Resource Center [сайт] / Gary Stoneburner, Alice Goguen, and Alexis Feringa; Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology. – Режим доступу: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (30.05.2012). – Назва з екрана. 3. Oleg Mikhail Sheyner. Scenario Graphs and Attack Graphs [Електронний ресурс] // SCHOOL OF COMPUTER SCIENCE, Carnegie Mellon [сайт] / Oleg Mikhail Sheyner. – Режим доступу: http://www.cs.cmu.edu/~scenariograph/sheynerthesis.pdf (30.05.2012). – Назва з екрана. 4. Абалмазов Э.И. Концепция безопасности: математический анализ эффективности. // Системы безопасности. – 1995. – № 1. 5. Кормен Т. Х. Алгоритмы: построение и аналіз. – 2-е изд.; пер. с англ. / Кормен Томас Х., Лейзерсон Чарльз И., Ривест Рональд Л., Штайн Клиффорд. – М.: Издательский дом "Вильямс", 2005. – 1296 с. 6. Introduction to lp_solve 5.5.2.0. – [Електронний ресурс] // lp_solve reference guide [сайт]. – Режим доступу: http://lpsolve.sourceforge.net/ (30.05.2012). – Назва з екрана. 7. Шутовський В.О. Розробка адаптивного алгоритму кількісної оцінки ризиків з використанням методів нечіткої логіки / В.О. Шутовський // "Теоретичні і прикладні проблеми фізики, математики та інформатики": зб. тез доп. учасників. – 2008. – С. 146. 8. Рутковский Л. Методы и технологии искусственного интеллекта / Л. Рутковский. – М.: Горячая линия - Телеком, 2010. – 520 с.*