легко інтерпретувати результати за допомогою причинно-наслідкових зв'язків (відношень) між концептами.

Список використаних джерел

1. Буров Є. Архітектура опрацювання знань у когнітивній інформаційній системі / Є. Буров // Вісник Національного університету "Львівська політехніка". – 2009. – № 650 : Комп'ютерні науки та інформаційні технології. – С. 28–37. – Режим доступу до ресурсу: http://vlp.com.ua/node/3952

2. Cognition [Електронний ресурс] – Режим доступу до ресурсу: https://www.answers.com/search?q=cognition.

3. Newell, A..Unified Theories of Cognition [Text]/ Newell A.- Harvard University Press.- Reprint edition, ISBN 0-674-92101-1.

4. Hollnagel, Erik, Joint cognitive systems : foundations of cognitive systems engineering [Text] / Erik Hollnagel and David D. Woods.- CRC Press, 2005.- ISBN 0-8493-2821-7.- 241p.

5. Борисов В. В. Нечеткие модели и сети / В. В. Борисов, В. В. Круглов, А. С. Федулов. – М.: Горячая линия - Телеком, 2007. – 284 с.

Стефанцев С.С., Ляшенко І.О.,
доценти кафедри
ДВНЗ «Київський національний економічний університет імені Вадима Гетьмана»
ingvar_la@ukr.net

КОГНІТИВНА КАРТА ОЦІНКИ РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В РОЗПОДІЛЕНИХ СИСТЕМАХ УПРАВЛІННЯ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Однією з обов'язкових умов успішної реалізації буд-якого інноваційного проекту є надійне забезпечення його інформаційної безпеки. На думку експертів з інформаційної безпеки, етап кореляції – як процесу інтерпретації, комбінації, порівняння та аналіз даних, які поступають від різних механізмів захисту інформації, вироблювані з метою визначення спроб несанкціонованого доступу до інформаційних ресурсів, є критичною частиною складного процесу аналізу загроз [1]. Аналіз сучасних методів дає змогу припустити, що найбільш зручним математичним апаратом для опису та дослідження оцінки ризику інформаційної безпеки в розподілених системах управління спеціального призначення є нечітке когнітивне моделювання.

Поняття нечіткої когнітивної карти (НКК) представляє собою розширення класичного поняття когнітивної карти, засноване на припущенні, що взаємовпливи між концептами можуть відрізнятися за інтенсивністю, і їх інтенсивність може змінюватися з плином часу **Error! Reference source not found.**[2]. Для цього в НКК вводять показник інтенсивності впливу і від класичного відносини переходять до нечіткого відношення *W*, елементи w_{ij} якого характеризують напрямок і ступінь інтенсивності (вагу) впливу між концептами e_i і e_j:

$$w_{ij} = w(e_i, e_j)$$

де w – нормований показник інтенсивності впливу (характеристична функція відносини W), яка володіє рядом спеціальних властивостей.

НКК відображає досліджуваний об'єкт у вигляді зваженого орієнтованого графа, вершини якого відповідають елементам множини E (концептів), а дуги – ненульовим елементам відносини W, тобто причинно-наслідковим зв'язкам. Кожна дуга має вагу, що задається відповідним значенням w_{ij}. Відношення W представляється у вигляді когнітивної матриці $W = \{w_{ij}, i, j = \overline{1,n}\}$ розмірності $(n \times n)$ (n – число концептів в системі), яка буде інтерпретуватися як матриця суміжності даного графа. Стан системи в поточний момент часу визначається набором значень всіх концептів НКК. Цільовий стан системи задається вектором значень множини цільових концептів.

В результаті опитування групи експертів виділяють n істотних чинників (концептів), що впливають на захищеність програмного забезпечення (ПЗ). Ці концепти розділимо на чотири групи (табл. 1). Для визначеності завдання дослідження скористаємося списком найбільш поширених уразливостей і неточностей ПЗ.

На наступному етапі на основі експертних оцінок визначають причинно-наслідкові зв'язки між концептами з виділенням їх спрямованості. Результатом таких дій є побудова когнітивної карти моделі формування ризику інформаційної безпеки у вигляді орієнтованого графа (рис. 1), що формально відбиває причинно-наслідкові зв'язки без урахування інтенсивності взаємовпливу концептів.

Таблиця 1

№ п/п	Найменування концепту	Концепт
А. Загрози		
1	Зовнішні атаки	e_1
2	Внутрішні (інсайдерські) атаки	e_2
Б. Дефекти програмного забезпечення		
3	Переповнювання буфера	e_3
4	Помилки при роботі з динамічною пам'ятю	e_4
5	Програмні закладки	e_5
6	Витоки даних; порушення цілісності інформаційних ресурсів	e_6
В. Технології захисту від реалізації вразливостей програмного забезпечення		
7	Захист на рівні компілятора	e_7
8	Спеціальні інструменти для захисту системних і прикладних ресурсів	e_8
9	Система обфускації (заплутування)	e_9
10	Контроль цілісності виконуваних програм на основі аналізу їх активності і їх оновлення	e_{10}
Г. Очікувані ефекти		
11	Якість функціонування програмного забезпечення	e_{11}
12	Ризики інформаційної безпеки, обумовлені порушенням працездатності програмного забезпечення	e_{12}

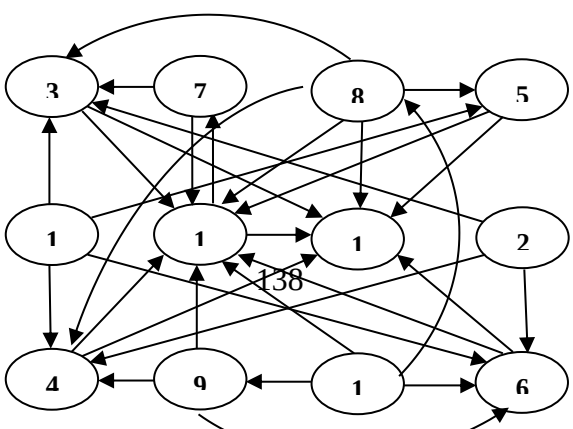

Рис.1. Когнітивна карта моделі формування ризику інформаційної безпеки

Висновок

Спираючись на результати проведеного когнітивного аналізу, можна припустити, що найбільший позитивний ефект слід очікувати від узгодженої зміни групи керованих концептів НКК, які знаходяться в ланцюжку причинно-наслідкового зв'язку і в сукупності забезпечують сталий вплив на систему – моделі формування ризику інформаційної безпеки.

Список використаних джерел

1. Гарусев М. Системы корреляции событий: революция или эволюция? / М. Гарусев // Сетевой online. 2003. – №7. – С. 7–11.

2. Силов В.Б. Принятие стратегических решений в нечеткой обстановке: монография. – М.: ИНПРО-РЕС, 1995. – 228 с.