УДК 004.056:519.816

Когнітивне моделювання як інструмент інформаційної безпеки

Аріна Гаркушенко[0009-0003-7568-7900]
Світлана Шевченко[0000-0002-9736-8623]

Київський столичний університет імені Бориса Грінченка, Україна

Анотація. У тезах розглядається когнітивне моделювання як інструмент управління інформаційними ризиками в контексті зростаючої динамічності та складності кіберзагроз. Зокрема розглянуто когнітивні карти як потужний інструмент для аналізу ризиків, виявлення уразливих місць у системі та оцінки ефективності засобів захисту. Розглянуто принцип їх функціонування, побудови, а також можливі переваги і недоліки. Приділено увагу можливості застосування нечітких когнітивних карт для прогнозування загроз та створення сценаріїв захисту. Представлено методику проведення тренінгу з моделювання поведінки атакуючих і внутрішніх користувачів у сценаріях з використанням нечітких когнітивних карт.
Ключові слова: інформаційна безпека, когнітивне моделювання, загрози, нечіткі когнітивні карти.

Cognitive Modeling as an Information Security Tool

Arina Harkushenko[0009-0003-7568-7900]
Svitlana Shevchenko[0000-0002-9736-8623]

Borys Grinchenko Kyiv Metropolitan University, Ukraine

Abstract. The paper considers cognitive modeling as a tool for managing information risks in the context of the growing dynamism and complexity of cyber threats. In particular, cognitive maps are considered as a powerful tool for analyzing risks, identifying vulnerabilities in the system and assessing the effectiveness of protection measures. The principle of their functioning, construction, as well as possible advantages and disadvantages are considered. Attention is paid to the possibility of using fuzzy cognitive maps for threat prediction and creating protection scenarios. A training methodology for modeling the behavior of attackers and internal users in scenarios using fuzzy cognitive maps is presented.
Keywords: information security, cognitive modeling, threats, fuzzy cognitive maps.

Вступ

Під потенційними ризиками ІБ ми розуміємо числову (словесну) функцію, яка описує ймовірність втілення загроз ІБ та величини збитку від їх реалізації внаслідок використання цими загрозами уразливостей активів з метою нанесення шкоди організації [1]. Основним принципом управління ризиками ІБ є безперервна оцінка та адаптація, що має на меті постійне оновлення як оцінок ризиків, так і стратегій їх усунення [2].

Традиційні підходи до оцінювання ризиків ІБ обмежені у можливості врахування нечітких зв’язків, впливу людського чинника та динамічної природи загроз. У цьому

контексті перспективним інструментом стає когнітивне моделювання, яке є корисним інструментом для виявлення уразливих місць в системах безпеки та оцінювання ефективних заходів для їх усунення, а також надає відповідальним особам інструмент для аналізу різних сценаріїв та обґрунтованого прийняття рішень. Візуалізація цього процесу здійснюється за допомогою нечітких когнітивних карт [3-4].

Метою дослідження є підвищення ефективності захисту інформації на основі аналізу ризиків інформаційної безпеки з використанням нечітких когнітивних карт.

Об'єктом дослідження є процес управління ризиками інформаційної безпеки в умовах невизначеності.

Предметом дослідження є методи когнітивного моделювання та їх застосування для аналізу та прогнозування ризиків у кібербезпеці.

Частковими завдання даного дослідження є розкриття сутності когнітивного моделювання з використанням нечітких когнітивних карт та принципів їх побудови.

Методи та моделі

Когнітивна карта складається з вершин (понять) та дуг (впливів), що формують сценарії розвитку ситуацій при зміні окремих факторів. На основі таких моделей можна досліджувати зміну загального рівня ризику в системі з урахуванням взаємозв’язків відповідно до певних загроз, уразливостей чи активів.

Нечіткі когнітивні карти (НКК) – це тип когнітивної карти, який використовує нечітку логіку для представлення та аналізу взаємозв'язків між різними змінними в системі. Основна ідея полягає в моделюванні компонентів системи (змінних або факторів) та того, як вони впливають один на одного, з метою розуміння та прогнозування поведінки системи в цілому [4].

Поняття представлені у вигляді вузлів, а причинно-наслідкові зв'язки представлені у вигляді дуг між вузлами в НКК. Вузли або поняття вказують на інформацію про досліджувану систему, таку як атрибути, характеристики, якості, змінні та стани [5]. Поняття можуть мати прямі або непрямі зв'язки між собою або не мати жодних зв'язків [6]. Зв'язки між вузлами можуть бути позитивними, негативними або нейтральними, виражаючи тип зв'язку між поняттями та ступінь причинно-наслідкового зв'язку. На рис. 1 показано приклад методу НКК з його компонентами.

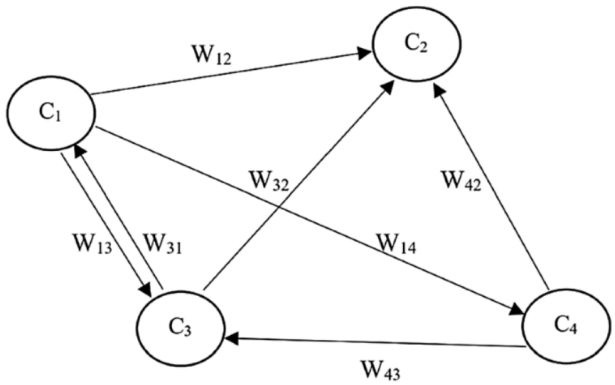

Рис. 1 Зразок НКК

C_i виражає вузли або поняття, пов'язані з зваженими дугами [7]. Кожен зв’язок між поняттями C_i та C_j має вагу W_{ij} (вага між вузлом i та вузлом j), яка може бути позитивною, негативною або нейтральною (вказує на те, що два поняття, що розглядаються, не мають зв'язку).

Після визначення значення вузла необхідно визначити інші вузли, пов'язані з цим вузлом, за допомогою рівняння (1):

$$A_i^{(k+1)} = f\left(A_i^{(k)} + \sum_{\substack{j=1 \\ j\neq i}}^{n} W_{ij} A_j^{(k)}\right) \quad (1),$$

де $A_i^{(k+1)}$ – значення концепції C_i в ітерації, $A_i^{(k)}$ – значення поняття C_i в ітерації, f(x) – функція перетворення.

Результати

Говорячи про розробку та застосування когнітивних карт у системах управління безпеки, можна виокремити такі практичні напрямки як формування сценаріїв кіберінцидентів на основі когнітивних моделей, оцінка ризиків на базі сценарного аналізу з урахуванням когнітивних факторів, моделювання поведінки атакуючих і внутрішніх користувачів у сценаріях, впровадження когнітивних сценаріїв у процес прийняття рішень (SOC, CERT) або ж автоматизація моніторингу та коригування ризиків за допомогою когнітивних моделей.

У даній роботі ми зупинились на одному з них, а саме створенні тренінгів з моделювання поведінки атакуючих і внутрішніх користувачів у сценаріях з використанням нечітких когнітивних карт. Обґрунтовано це тим, що такі тренінги безпосередньо підвищують готовність команд реагування, переводять теоретичні ризики в відпрацьовані сценарії реагування. Це підходить для більш обмежених даних, що робить реалізацію більш швидкою та реалістичною на початкових етапах, враховує невизначеності та причинно-наслідкові ланцюжки (сценарії внутрішньої взаємодії та поведінка під час атаки часто залежать від ледь помітних людських факторів (мотивація, доступ, стрес) – НКК корисні там, де причинно-наслідкові зв'язки нечіткі та взаємозалежні [8]), враховує інтерпретованість та навчання персоналу, що важливо для вміння практичного застосування і корекції сценаріїв у режимі реального часу в подальшому, а також має відносну простоту впровадження, що дозволяє швидко перейти від дослідження до практичної реалізації.

На початковому етапі важливо сформувати мету і цілі тренінгу. В нашому випадку це можливість виявляти ознаки інсайдерської або зовнішньої атаки на початкових етапах, відпрацювання стратегії і прийняття рішень та поліпшення координації групи аналітиків у умовах можливого тиску чи невизначеності.

Наступним етапом є визначення концептів НКК. В нашому випадку ми будуємо список концептів, розбитих на групи: технічні («вхід з незвичайної IP-адреси», «підозріла активність», «права доступу»), поведінкові/людські («мотивація», «емоційний стрес», «задоволення від роботи») та процесуальні («час реагування», «доступність аудитів», «політика найменших привілеїв»).

Після чого ми переходимо до збирання експертних даних, оцінок та визначення ваг. На цьому кроці проводяться воркшопи з аналітиками та менеджерами безпеки для того, щоб визначати зв’язки між концептами (наприклад, «зменшення задоволеності» призводить до «зростання ймовірності інсайдерської шкоди»), оцінювати силу впливу у нечітких термінах (наприклад, «низький/середній/високий» переходить у конкретні числові ваги або нечіткі множини). Після чого відбувається усереднення та узгодження експертних оцінок, яке можливе, наприклад, порівнянням декількох створених НКК і їх обговоренням на експертній сесії [9].

Наступним кроком ми записуємо, використовуючи вже отримані дані, матрицю W ($n \times n$) ваг зв’язків. Коли ми запускаємо ітерації оновлення стану, ми отримуємо

динамічний сценарій. Для тренінгу ми можемо використовувати кілька конфігурацій початкових станів, які відрізняються в різних сценаріях [10].

Далі ми переходимо до генерації сценаріїв. В нашому випадку ми формуємо сценарій А ((повільне внутрішнє шахрайство), початковими значеннями якого є «задоволеність» = низький, «доступ» = високий, «контроль» = низький. Модель показує поступове збільшення «коефіцієнта витоку» з часом) та сценарій В ((швидка зовнішня компрометація), початковими даними якого є «успішність фішингу» = високий, «спільне використання прав» = середній. Модель показує швидкий стрибок у «доступі» та «експорті даних»). Кожен сценарій відтворюється через ключові ітерації НКК, учасники аналізують проміжні стани та приймають на основі цього рішення.

Наступним етапом є інтерактивна сесія тренінгу, тобто тепер учасники отримують початкові спостереження (лог-події) та візуалізації НКК. Протягом ітерацій організатор чи ведучий тренінгу дає додаткові фактори або події, згідно чому учасники приймають рішення (наприклад, блокування, опитування користувачів, ігнорування), після чого обговорюють прогнозовані події і бачать наслідки своїх рішень у оновленій моделі.

Метриками оцінювання успішності та ефективності запропонованого тренінгу є кількість помилкових/позитивних рішень, покращення узгодженості дій у команді (згідно опитування чи оцінку експертів) та час виявлення загроз у різних сценаріях.

Далі ми розглянемо приклад створення простої НКК для тренінгу. У нашій спрощеній демонстраційній моделі ми розглянемо п’ять основних факторів (вершин):

- мотивація атакуючого (A1);
- рівень підготовки атакуючого (A2);
- необережність користувачів (U1);
- політика безпеки та навчання (U2);
- рівень загрози (R).

Після визначення основних компонентів ми переходимо до визначення зв’язків (ребер). У нашому випадку:

$A1 \rightarrow R$ (чим вища мотивація атакуючого, тим вищий ризик, вага +0,7);

$A2 \rightarrow R$ (чим більше підготовлений атакуючий, тим вищий ризик, вага +0,9);

$U1 \rightarrow R$ (необережність користувачів збільшує ризик, вага +0,6);

$U2 \rightarrow U1$ (навчання зменшує необережність, вага -0,8);

$U2 \rightarrow R$ (навчання знижує ризик, вага -0,5).

На основі цих даних створюємо матрицю ваг W для НКК:

	A1	A2	U1	U2	R
A1	0	0	0	0	0,7
A2	0	0	0	0	0,9
U1	0	0	0	0	0,6
U2	0	0	+0,8	0	0,5
R	0	0	0	0	0

На основі цього прописуємо можливі сценарії. Наприклад, у сценарії 1 «недостатнє навчання персоналу» ми маємо на меті показати як дефіцит політики і навчання (U2) підвищує необережність користувачів (U1) і в підсумку збільшує загальний рівень ризику (R). У сценарії 2 «високий рівень підготовки атакуючого» ми маємо на меті відпрацювати реагування та майстерно виконану швидку атаку, коли атакуючий має високі навички і може використати слабкі точки у безпеці системи, навіть якщо персонал має певні знання (U2 середнє). І у сценарії 3 «сильна політика безпеки та навчання» ми

показуємо як висока якість політики безпеки та навчання (U2) знижують необережність користувачів (U1) і у підсумку загальний ризик (R), навіть коли є помірна/висока загроза атакуючого. У цьому сценарії ми вчимо команду фокусуватись не лише на технічних аспектах захисту, а і на профілактичних.

На основі цих даних ми створюємо власне візуальну ілюстрацію карти, граф, де вузли (кола) – це наші фактори (A1, A2, U1, U2, R), стрілки – причинно-наслідкові зв'язки між вагами (позитивні – червоні, негативні – сині). Наприклад, стрілка від U2 до U1 з негативною вагою показує, що підвищення навчання персоналу знижує необережність.

Учасники тренінгу можуть змінювати значення вхідних факторів (A1, A2, U1, U2), запускати модель та спостерігати, як змінюється рівень ризику (R). Це дозволяє зрозуміти вплив поведінки користувачів, побачити різні траєкторії розвитку кіберінциденту та усвідомити важливість навчання персоналу та політик безпеки.

Обговорення

Когнітивне моделювання має низку переваг: дозволяє візуалізувати складні сценарії; забезпечує інтеграцію знань різних експертів. Однак є й обмеження: модель залежить від якості експертних оцінок; складність масштабування для великих систем; необхідна адаптація у разі швидких змін у середовищі загроз.

Порівняно з класичними методами (наприклад, SWOT-аналіз), когнітивні карти є більш динамічними та інформативними.

Висновки

Когнітивне моделювання є ефективним підходом для управління ризиками інформаційної безпеки, особливо в умовах невизначеності, який має свої переваги та недоліки. Моделі, розроблені на основі нечітких когнітивних карт, можуть використовуватись як основи для створення систем підтримки прийняття рішень в управлінні інформаційними ризиками. За допомогою когнітивного підходу можна створити детальну модель системи безпеки, яка показує, як усі її елементи взаємопов'язані, як вони впливають один на одного та які наслідки можуть виникнути в результаті різних подій. Проте треба відзначити, що при побудові необхідно враховувати якість експертних знань та масштабування системи задля уникнення хибних результатів.

Слід також зазначити, що великі моделі потребують значних обчислювальних ресурсів для обробки даних. Тому перспективними напрямками подальших досліджень є розробка адаптивних моделей, здатних до самонавчання, а також інтеграція нечітких когнітивних карт з іншими методами штучного інтелекту.

Подяки та гранти

Результати наукових досліджень були виконані в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№ 0122U200483, КСУБГ, м. Київ).

Джерела

1. Шевченко, С.М., Жданова, Ю.Д., Спасітєлєва, С.О. &; Складанний П.М. (2020) «Проведення swot-аналізу оцінювання інформаційних ризиків як засіб формування

практичних навичок студентів спеціальності 125 Кібербезпека». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(10) с. 158-168.

2. ДСТУ ISO/IEC 27005:2023 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки

3. Shevchenko S., Zhdanova Y., Kryvytska O., Shevchenko H., Spasiteleva S. (2024) Fuzzy cognitive mapping as a scenario approach for information security risk analysis Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. c. 356-362. ISSN 1613-0073

4. Шевченко, С., Жданова, Ю., Складанний, П., & Петренко, Т. (2024). «Нечіткі когнітивні карти як інструмент візуалізації сценаріїв реагування на інциденти в системах безпеки». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 417–429.

5. Aguilar J (2003) A dynamic fuzzy-cognitive-map approach based on random neural networks. Int J Computat Cogn 1(4):91–107

6. Kang I, Lee S, Choi J (2004) Using fuzzy cognitive map for the relationship management in airline service. Expert Syst Appl 26(4):545–555

7. Papageorgiou EI, Spyridonos PP, Glotsos DT, Stylios CD, Ravazoula P, Nikiforidis GN, Groumpos PP (2008) Brain tumor characterization using the soft computing technique of fuzzy cognitive maps. Appl Soft Comput 8(1):820–828

8. Sarmiento, I., Cockcroft, A., Dion, A. et al. Fuzzy cognitive mapping in participatory research and decision making: a practice review. Arch Public Health 82, 76 (2024). https://doi.org/10.1186/s13690-024-01303-7

9. Yoon, Byung Sung and Jetter, Antoine J., "Comparative Analysis for Fuzzy Cognitive Mapping" (2016). Engineering and Technology Management Faculty Publications and Presentations. 112.

10. Kosko B (1986) Fuzzy cognitive maps. Int J Man Mach Stud 24(1):65–75.