УДК 004

ПРИКЛАД НЕЧІТКОЇ ОНТОЛОГІЧНОЇ СТРУКТУРИ СЦЕНАРІЇВ ВИТОКУ ІНФОРМАЦІЇ ТА КІБ

О. В. Козленко[1]

[1]*Національний технічний університет України «Київський політехнічний інститут» імені Ігоря Сікорського, Фізико-технічний інститут*

Анотація

У статті пропонується варіант нечіткої онтології для аналізу комплексних систем захисту інформації (КСЗІ), яка орієнтується на найбільш поширені варіанти сценаріїв витоку інформації та на особливості культури інформаційної безпеки. Подібна структура має враховувати можливі елементи захисту від сценаріїв витоку інформації, визначені дослідженням даних щодо інцидентів та специфіку культури інформаційної безпеки і може використовуватися як основа для аналізу КСЗІ системи.

Ключові слова: нечітка онтологія, сценарії витоку інформації, культура інформаційної безпеки, загрози інформації

Вступ

Процес побудови комплексних систем захисту інформації (КСЗІ) у зв'язку з необхідністю високого рівня деталізації її структури, зокрема, виділення головних складових елементів, впливових факторів, відношень між ними, вимагає для аналізу та дослідження цієї структури застосування чіткої формалізованої концептуальної схеми. Саме такі особливості властиві онтологічному аналізу. Вперше визначення поняття онтології дане Т.Грубером [2] і означає специфікацію концептуалізації, де в якості концептуалізації виступає опис множини об'єктів предметної області та зв'язків між ними. Але такі онтології не можуть використовуватися в областях, де є нечітка інформація через неможливість оперувати відношення без чітких рамок. Одним з варіантів вирішення цієї проблеми є використання нечіткої онтології, яка містить в собі елементи нечіткої логіки у множинах концептів та відношень. Алгоритм побудови нечіткої онтології був запропонований Лі [4] у роботі, пов'язаной з випуском новин. Пізніше То [9] запропонував $FOGA$ ($Fuzzy\ Ontology\ Generation\ Framework$) для створення нечітких онтологій, який базується на теорії нечітких множин та FCA($Fuzzy\ Concept\ Analysis$). Компанія Verizon щорічно проводить дослідження в області безпеки інформації [12],[13],[14],[15] і вже не перший рік ділять інциденти витоку даних на дев'ять можливих сценаріїв. Ці сценарії допомагають визначити необхідні міри захисту для запобігання витоку інформації відповідно у кожному з них але не тільки від технічних засобів залежить безпека інформаційного середовища.

1. Теоретичні основи побудови нечіткої онтології

Нечітка онтологія виступає як доповнення до формальної онтології і, згідно [11], визначається як O_F=<C,P_F,R_F,A_F>, де $C = \{ c_1, c_2 , ... , c_i, ... , c_n \}$, $i = \overline{1,n}$, $n = CardC$ – скінченна множина концептів (понять) заданої предметної області. Кожен елемент множини має властивості, які є нечіткими множинами або значеннями. $P_F = \{ p_1, p_2 , ... , p_t \}$ – скінченна множина властивостей концептів предметної області. Властивість концепту $p \in P$,$p = (c, v_F, q_F, f, U)$, де відповідно $c \in C$ – концепт онтології, v_F – відображення властивості на c, q_F – лінгвістичні значення, які можуть впливати на v_F, f обмеження на v, U – область визначення. $R_F = \{ r_1, r_2 , ... , r_k, ... , r_m \}$, $k = \overline{1,m}$, $m = CardR_F$ – скінченна множина семантично значущих відносин між концептами предметної області. На відміну від формальної онтології, у випадку нечіткої онтології $r \in R_F$,$r = (c_1, c_2, t, s_F, U)$, де c_1, c_2 – концепти онтології, t – відношення між концептами, s_F – глибина відношення між концептами c_1 та c_2 , U – область визначення для нечітких концептів. A_F – множина нечітких правил. У нечітких онтологій A_F використовується як база знань. Таким чином, для побудови нечіткої онтології для елементів захисту інформації від витоку необхідно провести аналіз предметної області і виділити основні нечіткі концепти, відношення, аксіом та властивості.

2. Сценарії витоку інформації

Компанія Verizon щорічно проводить дослідження в області безпеки інформації [12],[13],[14],[15] і доводять доцільність поділу інцидентів витоку інформації на дев'ять можливих сценаріїв:

- вторгнення в точки продажу (POS – вторгнення)
- атаки на веб – застосунки
- злочинне ПЗ
- кібер – шпіонаж
- скимери платіжних карток
- фізична крадіжка або втрата

- різні помилки
- інсайдерські атаки
- DOS – атаки

Для визначення множини концептів нечіткої онтології нам необхідно провести аналіз кожного з цих сценаріїв У звітах про витоки даних в період за 2014 – 2017 роки компанія Verizon виділила відповідні загрози для кожного з вищезазначених сценаріїв. Спираючись на цю інформацію та фактори, які Verizon виділила у звіті про витоки інформації за 2014 рік [12] можливо визначити елементи захисту для вищезазначених сценаріїв:

- «Інвентаризація» ПЗ
- Відсутність непотрібного ПЗ, облікових записів, портів та ін.
- Оновлення та патчі
- Цілісність системних файлів
- Антивірусні програми
- Оновлення захисних програм
- DEP, $ASLR$, $EMET$
- Тестування веб – застосунків
- Закритість матеріалів для розробленого ПЗ
- Резервне копіювання
- Тренінги по ІБ для співробітників
- Перевірка працівників
- Фільтрування трафіку
- Відокремлення сервісів
- Контроль адміністраторів
- Складні паролі
- Відсутність паролів за замовчуванням
- Чорні та білі списки IP
- Подвійна автентифікація
- Протокол $Netflow$
- Журнал подій
- Аккаунт – менеджмент
- Централізована автентифікація
- Моніторинг входів
- Шифрування
- Відсутність конфіденційних даних у відкритому тексті
- DLP – система
- Робота з інцидентами
- Ролі при інцидентах
- Сегментація мережі
- Відео спостереження
- Перевірка терміналів
- Попередження користувачів
- Ефективний дизайн

Як зазначалося, не всі загрози безпосередньо залежать від технічних особливостей систем. Небезпеку також становить «людський фактор», який не завжди пов'язаний з нестачею або недосконалістю заходів захисту, але він завжди пов'язан з недотриманням вимог політики безпеки (ПБ)[6]. Як зазначено у [5] користувачі, умисно або через нестачу знання, є найбільшою загрозою для інформаційної безпеки. У роботі [7] Сіпонен зазначає, що без необхідних знань та співпраці користувачів з відділом безпеки або менеджменту адекватні засоби безпеки стають неефективними. У існуючій літературі культура інформаційної безпеки (КІБ) є важливою складовою у забезпеченні безпеки інформаційних активів організацій. У таких работах як [1] автор визначає КІБ як поведінку,цінності та припущення, які забезпечують безпеку інформації, дослідники у [3] визначають КІБ як систему, у якій взаємодіють мотивація, спрямування, знання та ментальні моделі. Ван Нікерк та Вон Солмс у своїй роботі [10] пропонують концептуальну модель культури інформаційної безпеки. Ця модель спрямована на визначення взаємодії між різними елементами, які складають культуру інформаційної безпеки. Досліди, які були проведені у [6],[9] допомагають розкласти поняття «КІБ» на складові. Тим самим, «КІБ» можливо визначити наступними складовими:

- «Персонал»
- «Кадрова безпека»
- «Міра прийняття КБ»
- «Керівництво»
- «Управлінська готовність»
- «Координованість»
- «Співпраця з відділом ІБ»
- «Співпраця з менеджментом»

Цей розклад ми й будемо використовувати для подальшого аналізу і побудови досліджуваної структури.

3. Побудова нечіткої онтології

Як було зазначено, для побудови онтології потрібно визначити основні множини. Проведений аналіз допоможе визначити основні елементи взаємодії та характеристики між заходами захисту від витоку інформації та заходами забезпечення належного рівня культури інформаційної безпеки. Основні значення найбільш важливих елементів , отриманих за допомогою попереднього аналізу наведені у таблиці 1. Для побудови нечіткої онтології будемо використовувати модифікований алгоритм, який зазначений у роботі [8], яка у свою основана на роботі [11]. Кожний з елементів захисту буде визначений за допомогою 5 характеристик: Цілі (G) — основні цілі реалізації атаки $G = 1$, якщо порушується тільки одна властивість захищеної інформації $G = 2$, якщо порушується дві властивості захищеної інформації $G = 3$, якщо порушується усі три властивості захищеної інформації Основні методи захисту (SM) — елементи захисту для запобігання реалізації витоку інформації за даної вразливості $SM = k$, $k \in [1, n]$, n – кількість елементів захисту Способи використання (W) — можливі способи реалізації загрози (локальні, дистанційні) $W = 1$, якщо загроза реалізується одним з способів (локальний або дистанційний) $W = 2$, якщо загроза може бути реалізована обома способами (локально та дистанційно) Критичність за кількості інцидентів (R_i) — параметр, який визначає вагу відносну критичності вразливості за кількостю інцидентів реалізації цієї загрози Критичність за кількістю реалізації витоку інформації (R_r) — параметр, який визначає вагу відносно критичності вразилвості щодо кількості реалізації витоку інформації за цією загрозою Визначення характеристик

та визначаються за допомогою формул

$$R_i = log_{10}(\sum incidents) \quad (1)$$

$$R_r = log_{10}(\sum leaks) \quad (2)$$

Статистика кількості інцидентів та витоків інформації взята з досліджень компанії Verizon за 2014 – 2017 роки [12],[13],[14],[15]. Через відсутність необхідної інформації щодо кількості інцидентів та витоків інформації стосовно культури інформації безпеки відповідні значення характеристик були взяті як середні значення від елементів, які пов'язані з культурою інформаційної безпеки (такі як «захист від інсайдерських атак» та інше) Формула визначення вагового коефіцієнту складається з

$$F = G * R * \frac{R_r}{R_i} \quad (3)$$

Значення, які характеристики, визначаються за допомогою вагової характеристики та кількості атрибутів кожної характеристики. Тим самим ці значення представляються за допомогою формули

$$F_r = F * W_p * i(SM) \quad (4)$$

де $i(SM)$ — кількість можливих спільних атрибутів між двома концептами. W_P— вагова характеристика, яка визначається як $W_P = (3, objective), (16, securitymeasures), (2, method)$
Тип звязку між двома концептами визначається наступною множиною: $T = weak, medium, good$ Відношення між концептами, як зазначалося у пункті 1, визначається через множину $r = (c_1, c_2, T, s_F, U)$. Множини c_1, c_2, s_F, U вже визначені . Множина сили відношення (s_F) спирається на визначення мінімальних та максимальних значень. Визначимо ці значення наступним чином:

$$S_{F_{min}} = W_P * min(i) \quad (5)$$

$$S_{F_{max}} = W_P * max(i) \quad (6)$$

Визначивши мінімальне та максимальні значення та маючи множину T,s_F будет складатися з наступних значень: S_F=[0 – 38,weak],[39 – 71,medium],[72 – 109,good] У даному прикладі в множину P будуть записані елементи з значеннями $medium$ та $good$ Відповідно множина P матиме вигляд (для найбільш значущих елементів) (Захист від атак на веб – застосунки, Захист від кібер – шпигунства,39,medium), (Захист від атак на веб – застосунки, Захист від злочинного ПЗ,45,medium), (Захист від DOS – атаки, Кадрова безпека,40,medium), (Захист від DOS – атаки, Міра прийняття КБ,40,medium), (Захист від DOS – атаки, Управлінська готовність,40,medium), (Захист від інсайдерськіх атак, Захист від різних помилок,37,medium), (Захист від інсайдерськіх атак, Управлінська готовність,37,medium), (Захист від кібер – шпигунства, Захист від злочинного ПЗ,71,medium), (Захист від кібер – шпигунства, Кадрова безпека,39,medium), (Захист від кібер – шпигунства, Міра прийняття КБ,39,medium), (Захист від злочинного ПЗ, Захист від POS – вторгнень,77,good),, (Захист від POS – вторгнень, Кадрова безпека,45, medium), (Кадрова безпека, Міра прийняття КБ,77,good), (Кадрова безпека, Управлінська готовність,109,good), (Міра прийняття КБ, Управлінська готовність,61, medium)

Висновки

В роботі було проаналізовані сценарії витоку інформації, які були отримані з звітів щодо витоку інформації за 2014 – 2017 роки та особливості культури інформаційної безпеки, яка має відношення до загроз, пов'язаних з людськими чинниками. В результаті проведеного аналізу було визначено необхідні множини та відношення для побудови нечіткої онтології. Отримана структура враховує можливі елементи захисту від сценаріїв витоку інформації, визначені дослідженням даних щодо інцидентів в області інформаційної безпеки та з врахуванням специфіки культури інформаційної безпеки. Як можна побачити у роботі, відношення між елементами захисту може бути одним значення з множини , що допомогає зробити висновок, що використання одного елементу захисту інформації з зазначених у роботі може призвести до використання елементу, який знаходиться з ним у відношенні. Ця структура може використовуватися як основа для аналізу КСЗІ системи.

Перелік використаних джерел

1. Dhillon G Managing information system security London: Macmillan — 1997. —
2. Gruber T.R. oward principles for the design of ontologies used for knowledge sharing. Hum.-Comput. Stud. — 1995. — № 43(5-6). – pp. 907-928.
3. Helokunnas T. nformation security culture in a value net. In: Engineering Management Conference, IEMC'03 on Managing Technologically Driven Organizations: The Human Side of Innovation and Change New York: IEEE Press. — 2003. — - pp. 190–194.
4. Lee C.S A fuzzy ontology and its application to news summarization IEEE Transactions on Systems, Man and Cybernetics (Part B). — 2005. — 35(5) –pp. 859- 880.
5. K.D. Mitnick , Simon W.L. The art of deception: controlling the human element of security Wiley Publishing. — 2002. — p. 3.
6. A.V. Potiy, D.Y. Pilipenko, I.N. Rebriy The prerequisites of information security culture development and an approach to complex evaluation of its level — 2012. – № 5 (57).— с.72 – 77.
7. Siponen M.T. Five dimensions of information security awareness Computers and Society. — 2001. — pp.24-9.
8. Tafazzoli T., S. H. Sadjadi Malware fuzzy ontology for semantic web International Journal of Computer Science and Network Security — 2008. — vol. 8 - pp. 157-159.

Табл. 1. Основні значення найбільш важливих елементів

Елемент	Запобігає порушеню	Основні методи захисту	Способи використання атаки	R_i	R_r
Захист від атак на веб – застосунки	КЦД	Тестування веб – застосунків, закритість матеріалів для розробленого ПЗ, оновлення та патчі, подвійна автентифікація	Дистанційний, локальний	4	3
Захист від DOS – атаки	КД	Робота з інцидентами, ролі при інцидентах, DLP – система	Дистанційний	4	0
Захист від інсайдерськіх атак	К	Журнал подій, аккаунт – менеджмент, централізована автентифікація, моніторинг входів, контроль адміністраторів, DLP – система, відсутність конфіденційних даних у відкритому вигляді	Локальні	4	2
Захист від різних помилок	КЦД	DLP – система, Відсутність конфіденційних даних у відкритому вигляді	Дистанціний, локальний	4	2
Захист від кібер – шпигунства	К	Тренінги по ІБ для співробітників, перевірка працівників, сегментація мережі, Інвентарізація ПЗ, Чорні та білі списки IP, Оновлення та патчі, Подвійна автентифікація	Дистанціний, локальний	3	3
Захист від злочинного ПЗ	КЦД	Інвентарцізація ПЗ, антивірусні програми, оновлення захисних програм, DEP, ASLR, EMET, чорні та білі списки IP, немає непотрібного ПЗ, облікових записів, портів, оновлення та патчі, цілісність системних файлів, подвійна автентифікація	Дистанційний, локальний	4	2
Захист від POS – вторгнень	КЦД	антивірусні програми, оновлення захисних програм, DEP, ASLR, EMET, фільтрування трафіку, журнал подій, протокол NetFlow, подвійна автентифікація, контроль адміністраторів, відокремлення сервісів, складні паролі, відсутність паролів за замовчуванням	Дистанційний, локальний	3	3
Кадрова безпека	КЦД	Складні паролі, відсутність паролів за замовчуванням, журнал подій, тренінги по ІБ для співробітників, перевірка працівників, робота з інцидентами, ролі при інцидентах	Дистанційний, локальний	4	2
Міра прийняття КБ	КЦД	ренінги по ІБ для співробітників, перевірка працівників, робота з інцидентами, ролі при інцидентах	Дистанційний, локальний	4	2
Управлінська готовність	КЦД	контроль адміністраторів, перевірка працівників, робота з інцидентами, ролі при інцидентах, складні паролі, відсутність паролів за замовчуванням, журнал подій	Дистанційний, локальний	4	2
Координованість	КЦ	співпраця з відділом ІБ, співпраця з менеджментом	Дистанційний, локальний	4	2

9. Q. T. Tho, S. C. Hui, A. C. M. Fong, T. H. Cao Automatic fuzzy ontology generation for semantic web IEEE Transactions on Knowledge and Data Engineering — 2006. — 18(6). – pp.842- 856.
10. J.F. Van Niekerk, R. Von Solms Information security culture: A management perspective IEEE Transactions on Knowledge and Data Engineering — 2010. — p.478.
11. J.Zhou, Y. Liang Fuzzy Ontology Model for Knowledge Management atlantis-press.com. — 2006. — pp.2-3.
12. 2014 Data Breach Investigation Report, Verizon Enterprise Solutions, 2014.
13. 2015 Data Breach Investigation Report, Verizon Enterprise Solutions, 2015.
14. 2016 Data Breach Investigation Report, Verizon Enterprise Solutions, 2016.
15. 2017 Data Breach Investigation Report, Verizon Enterprise Solutions, 2017.