© Kozlenko O. Building of fuzzy ontology for analysis of the information security system in ITS // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 3, pp. 156-162.

ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ОБЛАДНАННЯ / SOFTWARE & HARDWARE ARCHITECTURE SECURITY

DOI: 10.18372/2225-5036.24.12973

ПОБУДОВА НЕЧІТКОЇ ОНТОЛОГІЇ ДЛЯ АНАЛІЗУ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ІТС

Олег Козленко

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Україна

КОЗЛЕНКО Олег Віталійович

Рік і місце народження: 1993 рік, м. Ізмаїл, Одеська обл., Україна.
Освіта: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», 2016.
Посада: аспірант національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
Наукові інтереси : інформаційна безпека.
Email: education.kozlenko@gmail.com

Анотація. *У статті пропонується варіант нечіткої онтології для аналізу комплексних систем захисту інформації в ІТС, яка орієнтується на найбільш поширені варіанти сценаріїв витоку інформації та на особливості культури інформаційної безпеки. Результати реалізації загрози можуть впливати на інформацію як безпосередньо, так і опосередковано. Аналіз систем захисту інформації в ІТС спирається на багато факторів (сценарії атак на систему та інше) серед яких також можуть бути не тільки технічні засоби. Зазвичай загрози інформації в інформаційній системі залежать від характеристик внутрішньої системи, фізичного середовища, персоналу і оброблюваної інформації. Загрози можуть мати як об'єктивну складову (зміна умов фізичного середовища, відмова елементів взаємодії системи) так і суб'єктивну - «людський фактор», який не завжди пов'язаний з нестачею або недосконалістю заходів захисту, але він завжди пов'язан з недотриманням вимог політики безпеки. Звичайні помилки та нерозуміння визначення інцидентів безпеки та як на них реагувати теж грає важливу роль. Отже, для базової захищеності системи потрібно визначити багато факторів і структура, де буде визначено фактори, сценарії та зв'язок між елементами захисту для подальшого використання буде значно спрощувати розуміння та побудову системи захисту інформації в ІТС. Саме такі особливості властиві онтологічному аналізу, що базується на понятті «онтології». Але онтології за класичним визначенням не можуть використовуватися в областях, де є нечітка інформація через неможливість оперувати відношеннями 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. Дана онтологія може бути використана для сценаріїв витоку інформації з урахуванням культури інформаційної безпеки та для подальшого визначення загальної формальної оцінки захищеності організації.*

Ключові слова: *онтологія, нечітка онтологія, сценарії витоку інформації, культура інформаційної безпеки, загрози інформації, рівень культури інформаційної безпеки.*

Вступ

Процес побудови системи захисту ІТС 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. Такі особливості властиві онтологічному аналізу, що базується на понятті «онтології», але такі онтології не можуть використовуватися в областях, де є нечітка логіка . 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 [5] у роботі, пов'язаної з випуском новин. Пізніше То [10] запропонував FOGA (Fuzzy Ontology generation Framework) для створення нечітких онтологій, який базується на теорії нечітких множин та FCA (Fuzzy Concept Analysis). Задачею роботи є побудова нечіткої онтології сценаріїв витоку інформації та культури інформаційної безпеки. Метою роботи є визначення типів зв'язків між елементами системи захисту інформації в ІТС для можливого подальшого використання для формальної оцінки захищеності системи.

Теоретичні основи побудови онтології предметної області та нечіткої онтології

Якщо підходити до визначенням поняття «онтологія» за Грубером з формальної позиції, то згідно [3] під комп'ютерною онтологією предметної області розуміється : $O =< C, P, R, A >$, де :

– $C = \{c_1, c_2, \ldots, c_i, \ldots, c_n\}, i = \overline{1,n}$ – скінченна множина концептів (понять) заданої предметної області;

– $P = \{p_1, p_2, \ldots, p_t\}$ – скінченна множина властивостей концептів предметної області. Властивість концепту $p \in P, p = (c, f, v)$, де $c \in C$ – концепт онтології, v - відображення властивості на c, f – обмеження на v (тип, розмірність, границі та т.п.);

– $R = \{r_1, r_2, \ldots, r_k, \ldots, r_m\},, k = \overline{1,m}$ – скінченна множина семантично значущих відносин між концептами предметної області. У загальному випадку відносини ділять на загальнозначущі (з яких виділяють, як правило, відносини часткового порядку) і конкретні відносини заданої предметної області;

– $A = \{a_1, a_2, \ldots, a_j, \ldots, a_l\}, j = \overline{1,l}$ – скінченна множина аксіом. Аксіомою зазвичай виступає факт або правило.

Нечітка онтологія виступає як доповнення до формальної онтології і, згідно [12], визначається як $O_F =< C, P_F, R_F, A_F >$, де:

– $C = \{c_1, c_2, \ldots, c_i, \ldots, c_n\}, i = \overline{1,n}$ – скінченна множина концептів (понять) заданої предметної області. Кожен елемент множини має властивості, які є нечіткими множинами або значеннями;

– $P_F = \{p_1, p_2, \ldots, p_t\}$ - 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;

– $R_F = \{r_1, r_2, \ldots, r_k, \ldots, r_m\},, k = \overline{1,m}$ – 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.

Сценарії витоку інформації

Однією з складових аналізу інформаційних систем є визначення елементів комплексної системи захисту інформації в ІТС. Для визначення елементів захисту системи від витоку інформації потрібно знати можливі загрози для цільової системи та відповідно необхідні дії захисту. Згідно [1] дії, які призводять до реалізації потенційних небезпек, які у свою чергу ведуть до зниження цінності інформаційних ресурсів і мають потенційно можливий несприятливий вплив називаються загрозами, а спроба реалізації загрози називається атакою.

Компанія Verizon щорічно проводить дослідження в області безпеки інформації [13, 14, 15, 16] 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 та DOS-атаки [13, 14, 15, 16].

Для визначення множини концептів нечіткої онтології нам необхідно провести аналіз кожного з цих сценаріїв окремо:

– Сценарій «Вторгнення в точки продажу(POS-вторгнення)» містить в собі атаки на середовища, де проводяться роздрібні торгові операції.

– Сценарій «Атаки на веб-застосунки» – випадки з зловмисним кодом, спрямованим на вразливості рівня машинних команд у веб-додатках або зривом механізмів автентифікації.

– Сценарій «Злочинне ПЗ» – випадки заволодіння конфіденційною інформацією за допомогою програм зловмисників за виключенням випадків атак на точки продажу та на веб-застосунки.

– «Кібер-шпигунство» – інциденти, де мав місце неправомірний доступ до систем та мереж, пов'язаний з мотивом заволодіння чужою інформацією та/або мотивом шпигунства.

– Сценарій «Скимери платіжних карток» містить пристрої, фізично встановлені у місцях зчитування даних з магнітних стрічок платіжних карток, які збирають та дані та незаконно втручаються у платіжні операції.

– Сценарій «Фізична крадіжка або втрата» – це випадки крадіжки або загублення фізичних носіїв інформації.

– Сценарій «Різні помилки» – випадки ненавмисного компрометування атрибутів безпеки інформаційних активів, які зазвичай не мають під собою зловмисний мотив.

– Сценарій «DOS-атаки» містить атаки, які спрямовані на порушення доступності мережі або системи.

– Сценарій «Інсайдерських атак» охоплює всі інциденти зловживання внутрішніми працівниками або довіреними особами своїми правами чи свідомо недбале виконували своїх обов'язків.

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 [13], можливо визначити елементи захисту для вищезазначених сценаріїв:

– «Інвентаризація» ПЗ – ретельна перевірка типу, версій та номерів патчів всього ПЗ.

– Відсутність непотрібного ПЗ, облікових записів, портів та ін. – у системі відсутні ПЗ, облікових записів, відкритих портів та ін., що не використовується.

– Оновлення та патчі – оновлення та встановлення патчів для ПЗ та ОС.

– Цілісність системних файлів – перевірка підозрілих змін у системних файлах та появи нових підозрілих файлів у системних місцях , та звітування у разі знаходження такої активності.

– Антивірусні програми – ефективні антивірусні, анти-шпигунські програми та персональні брандмауери.

– Оновлення захисних програм – перевірка наявності оновлень для засобів захисту та їх своєчасне встановлення.

– DEP, ASLR, EMET – застосування технологій Data Execution Prevention (DEP), Address space layout randomization (ASLR) та Enhanced Mitigation Experience Toolkit (EMET).

– Тестування веб-застосунків – перевірка веб-застосунків на наявність потенційних вразливостей, помилок у коді, та ін.

– Закритість матеріалів для розробленого ПЗ – сторонні особи не мають доступ до матеріалів розробки (скрипти, невикористані бібліотеки та ін.).

– Резервне копіювання – процедура автоматичного резервного копіювання даних на постійній основі.

– Тренінги по ІБ для співробітників – обов'язкові навчальні заходи для співробітників.

– Перевірка працівників – періодичні тестування працівників.

– Фільтрування трафіку – фільтрування трафіку, що йде зі схвалених сервісів та портів.

– Відокремлення сервісів – відокремлення критично важливих сервісів системи від всіх інших сервісів (знаходиться фізично на іншій машині та мають окрему логіку).

– Контроль адміністраторів – системні адміністратори контролюються вищим керівництвом.

– Складні паролі – застосування складних паролів.

– Відсутність паролів за замовчуванням – заміна всіх паролів за замовчуванням.

– Чорні та білі списки IP – використання чорних списків з відомими зловмисними IP адресами або білих списків з довіреними IP адресами.

–Подвійна автентифікація – використання подвійної автентифікації.

–Протокол Netflow – облік мережевого трафіку.

–Журнал подій – перевірка та документування підозрілої активності в журналах подій.

–Аккаунт-менеджмент – переглядаються всі системні аккаунти та видаляються ті, що не асоціюються з жодним бізнес-процесом та власником.

–Централізована автентифікація – централізована точка автентифікації (наприклад LDAP, Active Directory).

–Моніторинг входів – перевірка входжень користувача у систему в нетиповий час або з перевищеною тривалістю.

–Шифрування – шифрування конфіденційної інформації спеціальними алгоритмами.

–Відсутність конфіденційних даних у відкритому тексті – сканування серверів на наявність конфіденційної інформації у форматі відкритого тексту.

–DLP-система – використання в мережі Data Leak Prevention (DLP) системи.

–Робота з інцидентами – інструкція для реагування працівників на інциденти.

–Ролі при інцидентах – призначення ролей та обов'язків конкретним співробітникам при реагуванні на інциденти.

–Сегментація мережі – виконується сегментація мережі на декілька довірених зон.

–Відео спостереження – використання засобів відео спостереження для контролю за подіями в терміналах, де використовуються кредитні картки.

–Перевірка терміналів – постійна перевірка стану терміналів, де використовуються кредитні картки на наявність загроз зчитування інформації з карток та інше.

–Попередження користувачів – вчасне попередження користувачів терміналів, де використовуються кредитні картки.

–Ефективний дизайн – створення елементів терміналів, які працюють з кредитними картками з використанням новітніх методів та засобів дизайну з точки зору безпеки.

Культура інформаційної безпеки

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'язаний з недотриманням вимог політики безпеки (ПБ)[7]. Як зазначено у [6] користувачі, умисно або через нестачу знання, є найбільшою загрозою для інформаційної безпеки. У роботі [8] Сіпонен зазначає, що без необхідних знань та співпраці користувачів з відділом безпеки або менеджменту адекватні засоби безпеки стають неефективними.

Дослідження людських чинників в області інформаційної безпеки все більше привертають увагу, тому що мають значний вплив на інформаційну безпеку в цілому і окремо на інсайдерську її складову. Згідно з результатами опитування, наведеними у [7], більшість співробітників впевнені, що відповідальність за цілісність інформаційних активів лежить на співробітниках інформаційної безпеки, головним завданням яких є усунення помилок і інцидентів.

У існуючій літературі культура інформаційної безпеки (КІБ) є важливою складовою у забезпеченні безпеки інформаційних активів організацій. У таких роботах як [2] автор визначає КІБ як поведінку, цінності та припущення, які забезпечують безпеку інформації, дослідники у [4] визначають КІБ як систему, у якій взаємодіють мотивація, спрямування, знання та ментальні моделі. Ван Нікерк та Вон Солмс у своїй роботі [11] пропонують концептуальну модель культури інформаційної безпеки. Ця модель спрямована на визначення взаємодії між різними елементами, які складають культуру інформаційної безпеки. Як зазначається у [7] рішення питання щодо дотримання вимог ПБ співробітниками може бути таким:

—Реалізація суворої системи перевірки, яка визначає систему штрафів і дисциплінарних заходів у разі недотримання. Це рішення дає швидкі результати, хоча негативне її сприйняття співробітниками робить цей ефект нетривалим.

—Розробка високого рівня КІБ. Варіант досить довгостроковий, але має тривалий ефект у разі успіху.

Досліди, які були проведені у [7,10] 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 онтології.

Побудова нечіткої онтології

Як було зазначено у пункті 1, для побудови онтології потрібно визначити основні множини. Проведений аналіз у пунктах 2 та 3 допоможе визначити основні елементи взаємодії та характеристики між заходами захисту від витоку інформації та заходами забезпечення належного рівня культури інформаційної безпеки. Основні значення, отримання за допомогою попереднього аналізу наведені у додатку 1. Для побудови нечіткої онтології будемо використовувати модифікований алгоритм, який зазначений у роботі [9], яка у свою основана на роботі [12]. 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: $SM = k$, $k \in [0, n]$, 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 кількістю інцидентів реалізації цієї загрози.

—Критичність за кількістю реалізації витоку інформації (R_r) — параметр, який визначає вагу відносно критичності вразливості щодо кількості реалізації витоку інформації за цією загрозою.

Визначення характеристик R_i та R_r визначаються за допомогою формул:

$$R_i = \left[log_{10} \left(\sum incidentsamount \right) \right];$$

$$R_r = \left[log_{10} \left(\sum leaksamount \right) \right].$$

Статистика кількості інцидентів та витоків інформації взята з досліджень компанії Verizon за 2014-2017 роки [13, 14, 15, 16]. 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

$$F = G * W * \left(\frac{R_i}{R_r} \right).$$

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

$$F_r = F * W_p * i(SM), i(SM) \in [0, n] ,$$

де $i(SM)$ – кількість можливих спільних атрибутів між двома концептами; W_p – вагова характеристика, яка визначається як

$$W_p = \{(3, objective), (16, measures), (2, method)\} .$$

Тип зв'язку між двома концептами визначається наступною множиною:

$$T = \{weak, medium, good\} .$$

Відношення між концептами, як зазначалося у пункті 1, визначається через множину R, елементи якої визначаються $r_i = (c_i, c_j, T, s_F, U)$. Елементи c_i, c_j, множини T та U вже визначені. Множина сили відношення (s_F) спирається на визначення мінімальних та максимальних значень. Визначимо ці значення наступним чином:

$$s_{Fmin} = count(min(weight)) * min(weight),$$

$$s_{Fmax} = W_p * max(i_n).$$

Визначивши мінімальне та максимальні значення та маючи множину T, s_F будет складатися з наступних значень:

$$[0-36]weak, [37-71]medium, [72-109]good.$$

Отже, множини P та R будуть складатися з:

– P ={(Захист від атак на веб-застосунки, {Тестування веб-застосунків, закритість матеріалів для розробленого ПЗ, оновлення та патчі, подвійна автентифікація}, {0, 128, 256, 384, 512}), (Захист від атак на веб-застосунки, {Конфіденційність, цілісність, доступність}, {0, 24, 48, 72}), (Захист від атак на веб-застосунки, {Дистанційний, локальний}, {0, 16, 32, 48}), (Захист від DOS-атаки, {Робота з інцидентами, ролі при інцидентах, DLP-система}, {0, 0, 0, 0}), (Захист від DOS-атаки, {Доступність, конфіденційність}, {0, 0, 0}), (Захист від DOS-атаки,{Дистанційний}, {0, 0}), (Захист від інсайдерських атак, {Журнал подій, аккаунт-менеджмент, централізована автентифікація, моніторинг входів, контроль адміністраторів, DLP-система, відсутність конфіденційних даних у відкритому вигляді}, {0, 96, 192, 288, 384, 480, 576, 672}), (Захист від інсайдерських атак, {Конфіденційність}, {0, 18}), (Захист від інсайдерських атак, {Локальні}, {0, 12}), (Захист від різних помилок, {DLP-система, Відсутність конфіденційних даних у відкритому вигляді}, {0, 192, 384}), (Захист від різних помилок,{Конфіденційність, цілістність, доступність},{0,36,72,108}), (Захист від різних помилок, {Дистанційний, локальний}, {0, 24, 48, 72}), (Запобігання фізичної крадіжки або втрат, {Резервне копіювання, шифрування, відсутність конфіденційних даних у відкритому вигляді}, {0, 32, 64, 96}), (Запобігання фізичної крадіжки або втрат, {Конфіденційність}, {0, 6, 12, 18}), (Запобігання фізичної крадіжки або втрат, {Локальний}, {0, 4, 8, 12}), (Захист від скримерів платіжних карток, {Відео-спостереження, перевірка терміналів, попередження користувачів, ефектиний дизайн}, {0, 16, 32, 48, 64}), (Захист від скримерів платіжних карток, {Конфіденційність}, {0, 3}), (Захист від скримерів платіжних карток, {Локальний}, {0, 2}), (Захист від кібер-шпигунства, {Тренінги по ІБ для співробітників, перевірка працівників, сегментація мережі, Інвентаризація ПЗ, Чорні та білі списки IP, Оновлення та патчі, Подвійна автентифікація}, {0, 32, 64, 96, 128}), (Захист від кібер-шпигунства, {Конфіденційність}, {0, 6}), (Захист від кібер-шпигунства, {Дистанційний, локальний}, {0, 4, 8}), (Захист від злочинного ПЗ, {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, {0, 192, 384, 576, 768, 960, 1152, 1344, 1536, 1728}), (Захист від злочинного ПЗ,{Конфіденційність, цілістність, доступність}, {0, 36, 72, 108}), (Захист від злочинного ПЗ, {Дистанційний, локальний}, {0, 24, 48}), (Захист від POS-вторгнень, {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}, {0, 96, 192, 288, 384, 480, 576, 672, 768, 864, 960}), (Захист від POS-вторгнень, {Конфіденційність, цілісність, доступність}, {0, 18, 36, 54}), (Захист від POS-вторгнень, {Дистанційний, локальний}, {0, 12, 24}), (Кадрова безпека, {Складні паролі, відсутність паролів за замовчуванням, журнал подій, тренінги по ІБ для співробітників, перевірка працівників, робота з інцидентами, ролі при інцидентах}, {0, 192, 384, 576, 768, 960, 1152, 1344}), (Кадрова безпека, {Конфіденційність, цілісність, доступність}, {0, 36, 72, 108}), (Кадрова безпека, {Дистанційний, локальний}, {0, 24, 48}), (Міра прийняття КБ, {Тренінги по ІБ для співробітників, перевірка працівників, робота з інцидентами, ролі при інцидентах}, {0, 192, 384, 576}), (Міра прийняття КБ, {Конфіденційність, цілісність, доступність}, {0, 36, 72, 108}), (Міра прийняття КБ,{Дистанційний, локальний}, {0, 24, 48}), (Управлінська готовність, {Контроль адміністраторів, перевірка працівників, робота з інцидентами, ролі при інцидентах, складні паролі, відсутність паролів за замовчуванням, журнал подій}, {0, 192, 384, 576, 768, 960, 1152, 1344}), (Управлінська готовність,{Конфіденційність, цілісність, доступність}, {0, 36, 72, 108}), (Управлінська готовність, {Дистанційний, локальний}, {0, 24, 48}), (Координованість, {Співпраця з відділом ІБ, співпраця з менеджментом}, {0, 192, 384}), (Координованість, {Конфіденційність, цілісність, доступність}, {0, 36, 72, 108}), (Координованість, {Дистанційний, локальний}, {0, 24, 48})}.

– R = {(Захист від атак на веб-застосунки, Захист від DOS-атаки, 8, weak), (Захист від атак на веб-застосунки, Захист від інсайдерських атак, 5, weak), (Захист від атак на веб-застосунки, Захист від різних помилок, 13, weak), (Захист від атак на веб-застосунки, Запобігання фізичної крадіжки або втрат, 5, weak), (Захист від атак на веб-застосунки, Захист від скримерів платіжних карток, 5, weak), (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 атак на веб-застосунки, Захист від POS-вторгнень, 29, weak), (Захист від атак на веб-застосунки, Кадрова безпека, 13, weak), (Захист від атак на веб-застосунки, Міра прийняття КБ, 13, weak), (Захист від атак на веб-застосунки, Управлінська готовність, 13, weak), (Захист від атак на веб-застосунки, Координованість, 13, weak), (Захист від DOS-атаки, Захист від інсайдерських атак, 19, weak), (Захист від DOS-атаки, Захист від різних помилок, 23,

weak), (Захист від DOS-атаки, Запобігання фізичної крадіжки або втрат, 3, weak), (Захист від DOS-атаки, Захист від скримерів платіжних карток, 3, weak), (Захист від DOS-атаки, Захист від кібер-шпигунства, 5, weak), (Захист від DOS-атаки, Захист від злочинного ПЗ, 8, weak), (Захист від DOS-атаки, Захист від POS-вторгнень, 8, weak), (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 DOS-атаки, Координованість, 8, weak), (Захист від інсайдерських атак, Захист від різних помилок, 37, medium), (Захист від інсайдерських атак, Запобігання фізичної крадіжки або втрат, 21, weak), (Захист від інсайдерських атак, Захист від скримерів платіжних карток,5,weak), (Захист від інсайдерських атак, Захист від кібер-шпигунства,5,weak), (Захист від інсайдерських атак, Захист від злочинного ПЗ, 5, weak), (Захист від інсайдерських атак, Захист від POS-вторгнень, 21, weak), (Захист від інсайдерських атак, Кадрова безпека, 21, weak), (Захист від інсайдерських атак, Міра прийняття КБ, 5, weak), (Захист від інсайдерських атак, Управлінська готовність, 37, medium), (Захист від інсайдерських атак, Координованість, 5, weak), (Захист від різних помилок, Запобігання фізичної крадіжки або втрат, 21, weak), (Захист від різних помилок, Захист від скримерів платіжних карток, 21, weak), (Захист від різних помилок, Захист від кібер-шпигунства, 7, weak), (Захист від різних помилок, Захист від злочинного ПЗ, 13, weak), (Захист від різних помилок, Захист від POS-вторгнень, 13, weak), (Захист від різних помилок, Кадрова безпека, 13, weak), (Захист від різних помилок, Міра прийняття КБ, 13, weak), (Захист від різних помилок, Управлінська готовність, 13, weak), (Захист від різних помилок, Координованість, 13, weak), (Запобігання фізичної крадіжки або втрат, Захист від скримерів платіжних карток, 5, weak), (Запобігання фізичної крадіжки або втрат, Захист від кібер-шпигунства, 5, weak), (Запобігання фізичної крадіжки або втрат, Захист від злочинного ПЗ, 5, weak), (Запобігання фізичної крадіжки або втрат, Захист від POS-вторгнень, 5, weak), (Запобігання фізичної крадіжки або втрат, Кадрова безпека, 5, weak), (Запобігання фізичної крадіжки або втрат, Міра прийняття КБ, 5, weak), (Запобігання фізичної крадіжки або втрат, Управлінська готовність, 5, weak), (Запобігання фізичної крадіжки або втрат, Координованість, 5, weak), (Захист від скримерів платіжних карток, Захист від кібер-шпигунства, 5, weak), (Захист від скримерів платіжних карток, Захист від злочинного ПЗ, 5, weak), (Захист від скримерів платіжних карток, Захист від POS-вторгнень, 5, weak), (Захист від скримерів платіжних карток, Кадрова безпека, 5, weak), (Захист від скримерів платіжних карток, Міра прийняття КБ, 5, weak), (Захист від скримерів платіжних карток, Управлінська готовність, 5, weak), (Захист від скримерів платіжних карток, Координованість, 5, weak), (Захист від кібер-шпигунства, Захист від злочинного ПЗ, 71, medium), (Захист від кібер-шпигунства, Захист від POS-вторгнень, 23, weak), (Захист від кібер-шпигунства, Кадрова безпека, 39, medium), (Захист від кібер-шпигунства, Міра прийняття КБ, 39, medium), (Захист від кібер-шпигунства, Управлінська готовність, 23, weak), (Захист від кібер-шпигунства, Координованість, 7, weak), (Захист від злочинного ПЗ, Захист від POS-вторгнень, 77, good), (Захист від злочинного ПЗ, Кадрова безпека, 13, weak), (Захист від злочинного ПЗ, Міра прийняття КБ, 13, weak), (Захист від злочинного ПЗ, Управлінська готовність, 13, weak), (Захист від злочинного ПЗ, Координованість, 13, weak), (Захист від POS-вторгнень, Кадрова безпека, 45, medium), (Захист від POS-вторгнень, Міра прийняття КБ,13,weak), (Захист від POS-вторгнень, Управлінська готовність, 13, weak), (Захист від POS-вторгнень, Координованість,13,weak), (Кадрова безпека, Міра прийняття КБ, 77, good), (Кадрова безпека, Управлінська готовність, 109, good), (Кадрова безпека, Координованість, 13, weak), (Міра прийняття КБ, Управлінська готовність, 61, medium), (Міра прийняття КБ, Координованість, 13, weak), (Управлінська готовність, Координованість, 13, weak)}.

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 онтологія 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 {*weak, medium, good*}, що допомагає зробити висновок, що використання одного елементу захисту інформації з зазначених у роботі може призвести до використання елементу, який знаходиться з ним у відношенні *medium* або *good* і навпаки. Ця структура може використовуватися як основа для аналізу системи захисту ІТС.

Література

[1]. О. Архипов, "Щодо методики ідентифікації та оцінювання активів системи інформаційних технологій", *Захист інформації*, № 1 (50), С. 42-47, 2011.

[2]. G. Dhillon, *Managing information system security*, London: Macmillan, 1997.

[3]. T. Gruber, "Toward principles for the design of ontologies used for knowledge sharing", *Int. J. Hum.-Comput. Stud.*, no. 43(5-6), pp. 907-928, 1995.

[4]. T. Helokunnas, R. Kuusisto, "Information 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*, pp. 190-194, 2003.

[5]. C.S. Lee, Z.W. Jian, L.K. Huang, "A fuzzy ontology and its application to news summarization", *IEEE Transactions on Systems, Man and Cybernetics (Part B)*, vol. 35(5), pp. 859-880, 2005.

[6]. K.D. Mitnick, W.L. Simon, "The art of deception: controlling the human element of security", Wiley Publishing, pp. 3-4, 2002.

[7]. A. Potiy, D. Pilipenko, I. Rebriy, "The prerequisites of information security culture development and an approach to complex evaluation of its level", *Радіоелектронні і комп'ютерні системи*, vol. 5, pp. 72-77.

[8]. M. Siponen, "Five dimensions of information security awareness", *Computers and Society*, pp. 24-29, 2001.

[9]. T. Tafazzoli, S. Sadjadi, "Malware fuzzy ontology for semantic web", *International Journal of Computer Science and Network Security*, vol. 8, pp. 157-159, 2008.

[10]. Q. Tho, S. Hui, A. Fong, T. Cao, "Automatic fuzzy ontology generation for semantic web", *IEEE Transactions on Knowledge and Data Engineering*, vol. 18(6), pp. 842-856, 2006.

[11]. J.F. Van Niekerk, R. Von Solms, "Information security culture: A management perspective", *Computers & Security*, pp.478-479, 2010.

[12]. J. Zhou, Y. Liang, "Fuzzy Ontology Model for Knowledge Management", pp. 2-3, 2006.

[13]. 2014 Data Breach Investigation Report, *Verizon Enterprise Solutions*, 2013.

[14]. 2015 Data Breach Investigation Report, *Verizon Enterprise Solutions*, 2014.

[15]. 2016 Data Breach Investigation Report, *Verizon Enterprise Solutions*, 2015.

[16]. 2017 Data Breach Investigation Report, *Verizon Enterprise Solutions*, 2016.

УДК 004.056.53

Козленко О. Построение нечеткой онтологии для анализа системы защиты информации в ИТС

Аннотация. *В статье предлагается вариант нечеткой онтологии для анализа комплексных систем защиты информации в ИТС, которая ориентируется на наиболее распространенные варианты сценариев утечки информации и особенности культуры информационной безопасности. Результаты реализации угрозы могут влиять на информацию как непосредственно, так и опосередковано. Анализ систем защиты информации в ИТС опирается на многие факторы (сценарии атак на систему и т.д.) среди которых также могут быть не только технические средства. Обычно угрозы информации в информационной системе зависят от характеристик внутренней системы, физической среды, персонала и обрабатываемой информации. Угрозы могут иметь как объективную составляющую (изменение условий физической среды, отказ элементов взаимодействия системы), так и субъективную - «человеческий фактор», который не всегда связан с недостатком или несовершенством мер защиты, но он всегда связан с несоблюдением требований политики безопасности. Обычные ошибки и непонимание определения инцидентов безопасности и как на них реагировать тоже играет важную роль. Итак, для базовой защищенности системы нужно определить многие факторы и структура, где будут определены факторы, сценарии и связь между элементами защиты для дальнейшего использования будет значительно упрощать понимание и построение системы защиты информации в ИТС. Именно такие особенности присущи онтологическому анализу, который основан на понятии «онтологии». Но онтологии по классическому определению не могут использоваться в областях, где есть нечеткая информация из-за невозможности оперировать отношениями без четких рамок. Одним из вариантов решения этой проблемы является использование нечеткой онтологии, которая включает в себя элементы нечеткой логики в множествах концептов и отношений. Данная онтология может быть использована для сценариев утечки информации с учетом культуры информационной безопасности и для дальнейшего определения общей формальной оценки защищенности организации.*

Ключевые слова: *онтология, нечеткая онтология, сценарии утечки информации, культура информационной безопасности, угрозы информации, уровень культуры информационной безопасности.*

Kozlenko O. Building of fuzzy ontology for analysis of the information security system in ITS

Abstract. *The article proposes a variant of the fuzzy ontology for the analysis of information security systems, which is based on the most common variants of information leaks scenarios and on the peculiarities of information security culture. Results of the implementation of the threat can affect the information both directly and indirectly. The analysis of information security systems is based on many factors (attack scenarios, etc.), which may include not only technical ways. Typically, threat information in the information system depends on the characteristics of the internal system, physical environment, personnel and information processed. Threats can have an objective component (changes in the physical environment, failure of elements of the interaction) and subjective - "human factor", which is not always associated with a deficiency or imperfection of security measures, but always associated with non-compliance with security policy requirements. Common mistakes and misunderstandings in identifying security incidents and how to respond to them is also important. Therefore, for the basic protection of the system, it is necessary to identify many factors and the structure, which will identify factors, scenarios and the relationship between the security elements for future use, will greatly simplify the understanding and construction of the information security system. It is these features that are inherent in ontological analysis, which is based on the concept of "ontology". But classical definition ontologies can not be used in areas where there is fuzzy information. One solution to this problem is to use a fuzzy ontology that contains elements of fuzzy logic in sets of concepts and relationships. This ontology can be used for information leaks scenarios, taking into account the culture of information security, and to further determine the overall formal assessment of the organization's security.*

Keywords: *ontology, fuzzy ontology, information leakage scenarios, information security culture, information threats, level of information security culture.*

Отримано 9 *вересня 2018 року*, затверджено редколегією *30 вересня 2018 року*