

# ПРИКЛАД ОНТОЛОГІЧНОЇ СТРУКТУРИ СЦЕНАРІЇВ ВИТОКУ ІНФОРМАЦІЇ ТА КУЛЬТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ АНАЛІЗУ КСЗІ

О. В. Козленко<sup>1</sup>

<sup>1</sup>Національний технічний університет України «Київський політехнічний інститут»

## Анотація

У статті пропонується варіант онтологічної структури для аналізу КСЗІ, яка орієнтується на найбільш поширені варіанти сценаріїв витоку інформації та на культуру інформаційної безпеки. Дана онтологічна структура може бути використана для визначення середнього значення ризику для сценаріїв витоку інформації та визначення рівня культури інформаційної безпеки.

**Ключові слова:** онтологічна структура, оцінювання ризику, сценарії витоку інформації, культура інформаційної безпеки

## Вступ

Компанії втрачають все більше конфіденційних даних, що спричиняє їм ще тяжчі збитки. Але компанії не мають достатньо внутрішньої інформації про витоки даних. Інформацію, яка доступна із зовнішніх ресурсів, також часто досить складно аналізувати через різноманітність сценаріїв та/або неповну інформацію про такі випадки. Ситуацію погіршує ще й той факт, що багато компаній намагаються приховати від медіа та контролюючих органів випадки компрометації даних, тому що це може значно зашкодити їх репутації. Аналіз КСЗІ спирається на багато факторів, таких як сценарії атак на систему та інше. Для розрахунку, наприклад, значення середнього ризику витоку інформації потрібно визначити багато факторів і структура, де буде визначено фактори та сценарії для подальшого використання буде значно спрощувати розуміння та автоматизацію цих розрахунків. Але не тільки від технічних засобів залежить безпека організації. Звичайні помилки та нерозуміння визначення інцидента безпеки та як на це реагувати теж грає важливу роль. Дана стаття фокусується на демонстрації структури, яку можна використовувати для аналізу КСЗІ та подальшого визначення загальної формальної оцінки захищеності організації та, як наприклад, автоматизації процесу визначення цієї оцінки, використовуючи цю структуру.

## 1. Сценарії витоку інформації

З точки зору захищеності інформації, інформація має 3 основні властивості: конфіденційність, цілісність і доступність, а загрози, реалізація яких призводить до втрати інформацією будь-якої з вищезазначених властивостей, відповідно називаються загрозами конфіденційності, цілісності та доступності інформації. Результати реалізації загрози можуть

впливати на інформацію як безпосередньо, так і опосередковано. Зазвичай загрози інформації в ІТС 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 (помилки персоналу або дії зловмисника). Загрози, що мають суб'єктивну основу, можуть бути випадковими або навмисними. Ідентифікація загроз (визначення множини загроз, реалізація яких можлива в конкретній ІТС) передбачає розгляд джерел впливів і наслідків реалізації загроз, а також їх класифікацію. Всі джерела загроз інформації можна розділити на три основні групи:

- загрози, зумовлені діями суб'єкта;
- загрози, зумовлені технічними засобами;
- загрози, зумовлені стихійними джерелами.

Перша група є найширшою та становить найбільший інтерес з точки зору організації захисту від загроз даного типу, так як дії суб'єкта завжди можна оцінити, спрогнозувати і вжити адекватних заходів. Методи і заходи протидії цим загрозам (контрзаходи) керовані і безпосередньо залежать від розробників СЗІ. Друга група містить загрози, безпосередньо залежні від властивостей. Технічні засоби, що містять канали реалізації потенційних загроз захищеності інформації, також можуть бути внутрішніми. Третю групу складають загрози, які абсолютно не піддаються прогнозуванню і тому заходи для їх запобігання повинні застосовуватися, по можливості, завжди, але не обов'язково до ІТС як до об'єкта захисту, а ширше, до всіх елементів технічної інфраструктури підприємства чи організації. Відсутність систем захисту корпоративної інформації, а також політики безпеки на підприємстві може стати причиною серйозних наслідків для бізнесу. Однак, хоча багато роботодавців розуміють, що система захисту

потрібна для підприємства, мало хто розуміє для яких саме цілей [1]. Першим таким інцидентом є промислове шпигунство. Потенціальними жертвами промислового шпигунства зазвичай виступають підприємства, що володіють або створюють якусь інтелектуальну власність. Основна загроза – втрата конкурентної переваги через втрату конфіденційної інформації. Наступним інцидентом є витік персональних даних. Від того наскільки великим та за яких обставин він стався, залежить розмір штрафу від регуляторів. Також витік персональних даних має негативний вплив і на співробітників. Іншою причиною витоку даних можуть стати недобросовісні працівники. Компанія у будь-яку мить може постраждати від примітивного шахрайства або якої-небудь іншої внутрішньої проблеми, наприклад зараження вірусом корпоративної системи. Зазвичай такі випадки не підлягають розголошенню щоб не зашкодити репутації компанії. Проте ображений співробітник заради помсти компанії може відкрити таку інформацію громадськості [2]. Verizon вже не перший рік проводить дослідження і, дивлячись на результати, доводять доцільність поділу інцидентів розголошення даних на дев'ять шаблонів сценаріїв: вторгнення в точки продажу (POS-вторгнення), атаки на веб-застосунки, злочинне ПЗ, кібер-шпionаж, скімери платіжних карток, фізична крадіжка або втрата, різні помилки, інсайдерські атаки та DOS-атаки [3, 4]. Аналіз інцидентів багатьох різних років довів, що таке розмежування сценаріїв є точним незалежно від того, як мінялася кількість випадків кожного з них.

## 2. Культура інформаційної безпеки

Нещодавні аналітичні звіти свідчать про те, що організації з різним напрямком діяльності (комерційні, урядові, академічні) потерпають від інцидентів безпеки, причиною яких є діяльність власних співробітників. Згідно [5] інциденти безпеки, причиною яких є людський чинник, не завжди пов'язані із нестачею або недосконалістю заходів захисту, а з недотриманням вимог політики безпеки (ПБ). Сприйняття ПБ як обмеження і незручності працівниками ускладнює виконання професійних обов'язків і це призводить до формування низького рівня культури інформаційної безпеки (КІБ). Важливо відзначити, що існує багато визначень терміна культури інформаційної безпеки. Узагальнюючи, можна сказати, що КІБ є набором цінностей, людських переконань, думок і моделей поведінки, які забезпечують певний ступінь відповідності вимогам ІБ в організації [5]. КІБ завжди має місце в організації і завжди має вплив на цю організацію, позитивну або негативну. Також є фактори, які впливають на вибір поведінки працівником, а саме нормативні переконання і встановлені норми поведінки. Нові працівники знаходяться в фазі адаптації та керуються встановленими нормами поведінки в першу чергу, з поступовим переходом до стандартної поведінки в трудовому колективі. Діяльність працівників, таким чином, регулюється шляхом

прийняття організаційної культури. Але КІБ сама по собі може розглядатися як продукт діяльності колективу. Якщо процес просування КІБ здійснюється спонтанно, це робить стандарти поведінки більш значущими і це демонструє негативний ефект в разі низької якості КІБ. Працівник приймає ідею бажаної та некоректної поведінки в процесі соціалізації. Цей процес допомагає співробітнику прийняти встановлені закономірності поведінки і стандарти організації (незалежно від їх відповідності вимогам ІБ). Згідно [5] «КІБ», визначається показниками «Персона» та «Керівництво». Індикатор «Персонал» визначається нижчими показниками «Кадрова безпека» і «Міра прийняття КБ», «Керівництво» – «Управлінська готовність» та «Координованість». Індикатор «Координованість» аналогічним чином визначається показниками нижчими рівня «Співпраця з відділом ІБ» і «Співпраця з менеджментом».

## 3. Онтологія предметної області

Структура для аналізу КСЗІ з вищезазначених факторів та з урахуванням рівня культури інформаційної безпеки повинна мати високий рівень деталізації формалізації за допомогою концептуальної схеми, через те, що може дуже багато визначень й відношень між ними. Якраз такі особливості властиві таким структурам як «онтології». Серед фахівців, що займаються проблемами комп'ютерної лінгвістики, найбільш усталеним (класичним) вважається визначення онтології дане Губертом: «онтологія – це специфікація концептуалізації» [6]. Так само відомий ряд розширених визначень Губерта, серед яких можна виділити такі:

- онтологія – це специфікація концептуалізації, де в якості концептуалізації виступає опис множини об'єктів предметної області та зв'язків між ними [7];
- онтологія – це знання, формально представлені на базі концептуалізації. Формально онтологія складається з термінів, організованих в таксономії їх визначень і атрибутів, а також пов'язаних з ними аксіом і правил поведінки [7];

Також є складності з формальним визначенням поняття «онтологія». Згідно [8] комп'ютерна онтологія предметної області (Пдо) це трійка:  $O = \langle X, R, F \rangle$ , де  $X = \{x_1, x_2, \dots, x_i, \dots, x_n\}$ ,  $i = \overline{1, n}$ ,  $n = \text{Card } X$  – кінцева множина понять заданої предметної області;  $R = \{r_1, r_2, \dots, r_k, \dots, r_m\}$ ,  $R : x_1 \times x_2 \times \dots \times x_n$ ,  $k = \overline{1, m}$ ,  $n = \text{Card } R$  – кінцева множина семантично значущих відносин між концептами Пдо і визначають тип взаємодії між поняттями.  $F : X \times R$  – кінцева множина функцій інтерпретації, заданих на  $X$  або  $R$ . У простому випадку методика проектування онтології Пдо включає три етапи проектування:

- 1) попередній аналіз заданої предметної області.
- 2) побудова вручну онтографа Пдо.
- 3) графічне (візуальне) проектування онтографа Пдо.

Онтограф – односпрямований орієнтований граф, в одну вершину якого може входити і виходити кілька

дуг, де вершинами є поняття предметної області, а дугами – зв'язки між ними.

Побудуємо онтологічну структуру системи для аналізу КСЗІ, беручи за основу матеріали по вищезазначеним сценаріям по витоку інформації та рівню культури ІБ. Першим та другим етапом є «Попередній аналіз заданої предметної області» та «Побудова вручну онтографа Пдо». Для цього потрібно зробити визначення множин  $X$  та  $R$  та зробити ранжування множини  $X$  по рівням по узагальненому відношенню «вище-нижче». Отже множина понять  $X$  (з урахуванням ранжування по рівням) буде мати вигляд:

- 1) Центр безпеки
- 2) Конфіденційні дані, Політика безпеки, КІБ.
- 3) Захист від витоку інформації, Персонал, Керівництво.
- 4) Атаки на веб-застосунки, DoS-атаки, Інсайдерські атаки, Різні помилки, Фізична крадіжка або втрата, Скримери платіжних карток, Кібершпиунство, Злочинне ПЗ, POS вторгнення, Управлінська готовність, Координованість.
- 5) Співпраця з відділом ІБ, Співпраця з менеджментом, Кадрова безпека, Міра прийняття КБ, Захист від шкідливого ПЗ, Фільтрування трафіку, Журнал подій, Протокол NetFlow, Подвійна автентифікація, Контроль адмінів, Відокремлення серверів, Паролі, Інвентаризація ПЗ, Чорні та білі IP списки, Конфігурація, Подвійна автентифікація, Обізнаність співробітників, Сегментація мережі, Інвентаризація ПЗ, Оновлення та патчі, Відео спостереження, Перевірка терміналів, Попередження користувачів, Ефективний дизайн, Резервне копіювання, Шифрування, DLP-Система, Журнал подій, Управління аккаунтами, Відсутність конфіденційних даних, Відповіді на інциденти, Безпека розробки.

Множина відношень  $R$  складається з відношень: {«Ціле-частина», «Визначає», «Використовує»}. Третім та остаточним етапом в побудові онтологічної структури є «Графічне (візуальне) проектування онтографа Пдо», яке зображено на рис. 1 та рис. 2.

## Висновки

Була отримана онтологічна структура (рис. 1 та рис. 2) системи для аналізу КСЗІ, яка враховує можливі сценарії по витоку інформації, які визначені дослідженням даних щодо інцидентів в області інформаційної безпеки та з врахуванням специфіки культури інформаційної безпеки. Цей онтограф може використовуватися як основа для визначення середнього ризику по байєсовському методу та визначення рівня культури інформаційної безпеки.

## Перелік використаних джерел

1. Архипов О.Є. Щодо методики ідентифікації та оцінювання активів системи інформаційних технологій / О.Є. Архипов // Захист інформації. — 2011. — №1 (50). — с.42–47.
2. Тимошенко А.А. Текст лекцій «Защита информации в специализированных информационно-телекоммуникационных системах» — — Киев, 2011. —
3. 2015 Data Breach Investigation Report, Verizon Enterprise Solutions, 2015.
4. 2014 Data Breach Investigation Report, Verizon Enterprise Solutions, 2014.
5. 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.
6. Gruber T.R. A translation approach to portable ontologies Knowledge Acquisition. — 1993. — № 5(2). — 199–220с.
7. Никоненко А.А. Обзор баз знаний онтологического типа «Искусственный интеллект» — 2004. — № 4. — 208–219с.
8. Палагин А.В., Петренко Н.Г. Методика проектирования онтологии предметной области // УСИМ. — 2009. — 14 с.

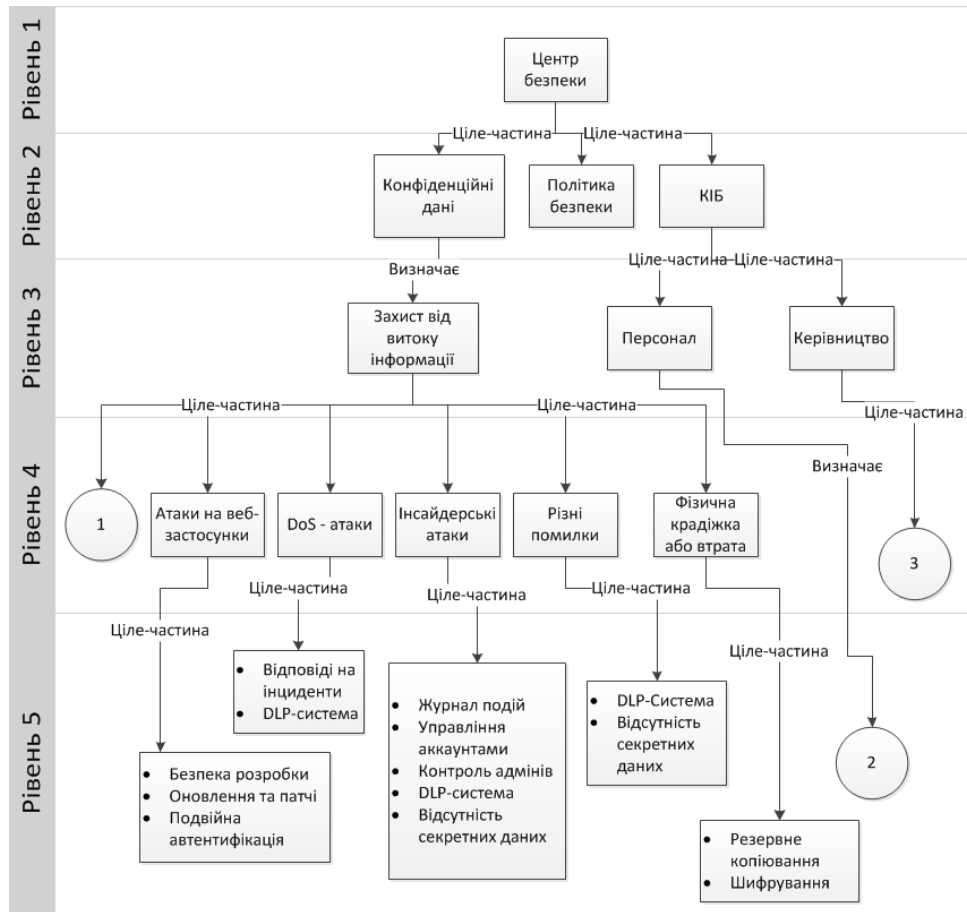


Рис. 1. Онтограф. Частина 1

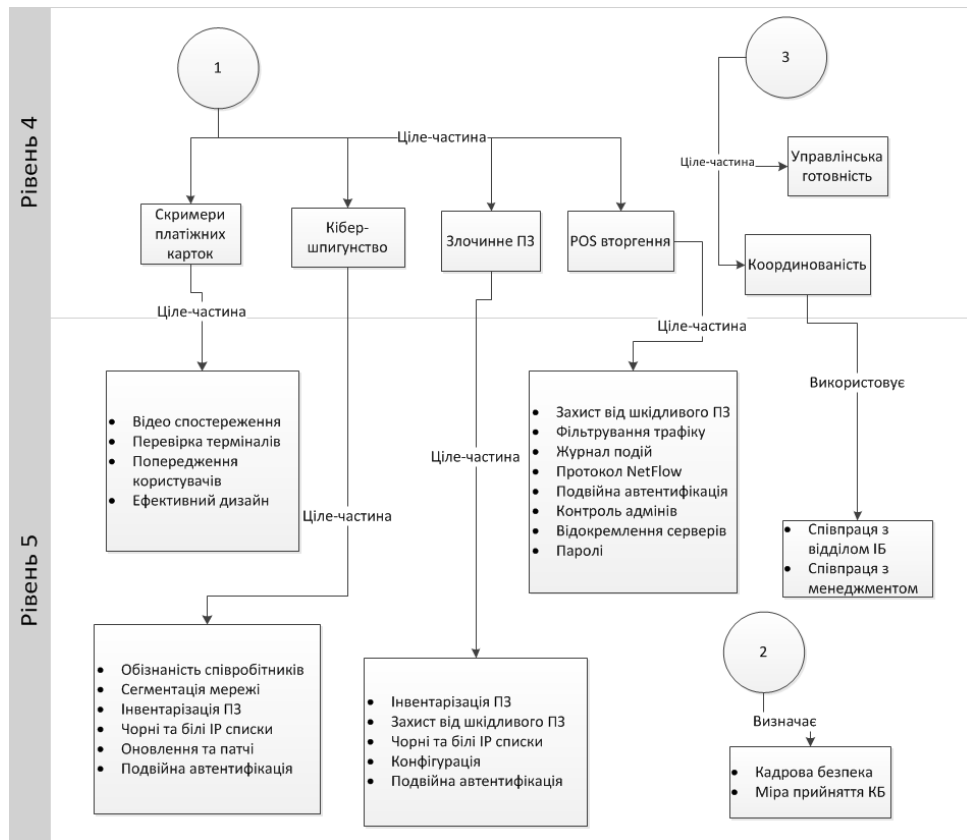


Рис. 2. Онтограф. Частина 2