

НАУКОВИЙ АВТОРСЬКИЙ КОЛЕКТИВ

Miskinis A., doctor of social sciences (розділ 3.7); Вітлінський В.В., д.е.н., професор (розділи 2.2, 2.3); Діордіца С.Г., д.е.н., професор (розділ 1.4); Захарченко П.В., д.е.н., професор (розділ 1.5); Іванов М.М., д.е.н., професор (розділ 2.5); Кібальник Л.О., д.е.н., доцент (розділ 1.6); Курбанов К.Р., д.т.н., професор (розділ 3.5); Лакіс В.Ю., д.е.н., професор (розділ 3.6); Порохня В.М., д.т.н., д.е.н., професор (розділ 3.8); Рамазанов С.К., д.т.н., д.е.н., професор (розділ 1.7); Таушанжи К.П., д.е.н., доцент (розділ 3.9); Соловійов В.М., д.ф.-м.н., професор (розділи 1.1, 2.4); Тюфекчи Фередун, д.е.н. (розділ 3.9); Черняк О.І., д.е.н., професор (розділ 1.9)

Dzemydaite G., doctor of social sciences (розділ 3.1); Lauzadyte-Tutliene A., doctor of economics and management, associate professor (розділ 3.3); Paliulyte R., dr., associated professor (розділ 3.2); Rasteniene A., dr., associated professor (розділ 3.2); Баженова О.В., к.е.н., доцент (розділ 3.4); **Бєгун А.В., к.е.н., професор (розділ 2.1)**; Гострик О.М., к.е.н., доцент (розділ 1.2); Гриценко К.Г., к.т.н., доцент (розділ 1.3); Данильчук Г.Б., к.е.н. (розділ 2.4); **Ігнатова Ю.В., к.е.н. (розділ 2.1)**; Кобець В.М., к.е.н., доцент (розділ 1.4); Меньяйлова Г.Є., к.е.н., доцент (розділ 3.5); **Осипова О.І., к.е.н. (розділ 2.1)**; Пушкар О.І., к.е.н. (розділ 3.5); Скіцько В.І., к.е.н., доцент (розділ 2.3); Соловійова В.В., к.е.н., доцент (розділ 1.2); Тішков Б.О., к.е.н., доцент (розділ 1.8); Шерстенников Ю.В., к.ф.-м.н., доцент (розділ 3.8)

Водолюєва І.Є. (розділ 1.1); Засядько О.А. (розділ 2.4); Котлярова Ю.О. (розділ 1.8); Кузьмич Н.В. (розділ 1.6); Лазаренко А.О. (розділ 1.1); Якимчук Б.Б. (розділ 1.9)

РОЗДІЛ 2 РИЗИК-МЕНЕДЖМЕНТ ТА БЕЗПЕКОЛОГІЯ ІННОВАЦІЙНОЇ ЕКОНОМІКИ

2.1. СИТУАЦІЙНЕ УПРАВЛІННЯ ЦЕНТРОМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В статті розглянуто задачу ситуаційного управління центром інформаційної безпеки на основі теорії прецедентів (Case Based Reasoning, CBR). Визначено, що методологія CBR є підходом, що дозволяє вирішити нову задачу, використовуючи або адаптуючи рішення вже відомої задачі. Виникаючі з плином часу ситуації й їхні методи вирішення зберігаються в спеціальній базі прецедентів. Коли виникає нова ситуація в базі прецедентів знаходять схожу ситуацію і метод її вирішення адаптується до ситуації, що розглядається.

В статті наведена ілюстрація реалізації моделі ситуаційного управління у Центрі інформаційної безпеки (ІБ), а також контрольний приклад взаємодії домену безпеки та Центру з вирішення ситуації інциденту. В свою чергу, це дозволило виділити наступні проблеми: необхідність роботи досвідчених експертів з управління інцидентами ІБ в доменах безпеки; ризик прийняття помилкового рішення при управлінні інцидентом ІБ; відсутність централізованого джерела статистики за інцидентами ІБ.

Ключові слова: теорія прецедентів, інформаційна безпека, база прецедентів, ситуаційне управління.

Вступ. У сфері управління інформаційною безпекою, де важливою складовою є швидкість та адекватність реакції на постійно виникаючі загрози інформаційного об'єкту, розглядається здатність використання ситуаційного підходу до її керування. При застосуванні ситуаційного підходу до управління інформаційною безпекою організації згідно з її політикою здійснюється моніторинг інформаційної безпеки (ІБ). За допомогою моніторингу відбувається процес постійного спостереження за подіями ІБ з метою своєчасного виявлення та реагування на ті з них, які призвели або можуть

призвести до реалізації загроз ІБ.

Розглядаючи ситуаційне управління як метод управління складними технічними і організаційними системами, на практиці використовуються: а) логіко-лінгвістичні моделі для рівня представлення знань про об'єкт управління і способи управління ним; б) моделі навчання в якості основних процедур при побудові процедур управління поточними ситуаціями; в) моделі дедуктивних систем для побудови багатокрокових рішень. Одним із ефективних засобів, який залучає запропоновані моделі в загальний процес дослідження, є використання елементів теорії прецедентів.

З розвитком теорії ситуаційного управління практика показала, що при виникненні нової проблемної ситуації доцільно використовувати метод міркувань на основі прецедентів (Case Based Reasoning, CBR).

Метод CBR виник з досліджень в когнітивній науці, і перш за все, в дослідженнях з динамічної пам'яті Роджера Шенка [1] і його учнів в Єльському університеті. Було встановлено, що люди зазвичай вирішують проблеми, спираючись на свій попередній досвід, пам'ятаючи, як вони вирішували подібні проблеми в минулому. Методологія CBR є підходом, що дозволяє вирішити нову задачу, використовуючи або адаптуючи рішення вже відомої задачі. Розуміння універсальності й широких можливостей цього підходу призвело до створення і швидкого розвитку теорії прецедентів [2].

Сутність методології CBR полягає в наступному. Прецедент є парою «ситуація» та «метод рішення». Виникаючи з плином часу ситуації й їхні методи вирішення зберігаються в спеціальній базі прецедентів. Коли виникає нова ситуація в базі прецедентів знаходять схожу ситуацію і метод її вирішення адаптується до ситуації, що розглядається.

Методологія CBR здійснюється у вигляді циклічної процедури, що складається з таких чотирьох процесів, які ще називаються «4Re-процеси» (рис. 1):

- 1) Retrieve: пошук схожого прецеденту для конкретного інциденту;
- 2) Reuse: застосування методу рішення прецеденту до конкретної ситуації;

3) Revise: перевірка отриманого рішення і адаптація рішення при необхідності;

4) Retain: збереження отриманого рішення в базі прецедентів для подальшого використання.

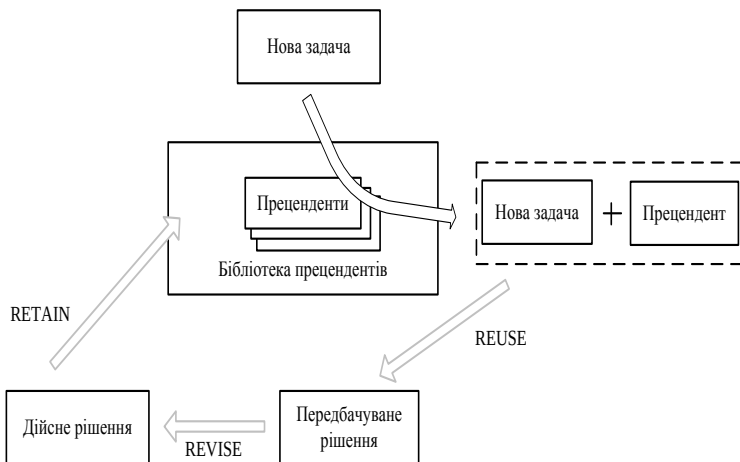


Рис. 1. Циклічні процедури «4Re-процеси»

Джерело: [1]

До переваг міркувань на основі прецедентів можна віднести наступні аспекти:

- можливість безпосередньо використовувати досвід, накопичений системою без інтенсивного залучення експерта в тій чи іншій предметній області;
- спроможність скорочення часу пошуку вирішення поставленого завдання за рахунок використання вже наявного рішення для такого завдання;
- існує здатність виключити повторне отримання помилкового рішення;
- відсутня необхідність повного та поглибленого розгляду знань про конкретну предметну область.

Зворотній зв'язок, який виникає при збереженні рішень для нових проблем, означає, що CBR-метод за сутністю є «самонавчальною» технологією, завдяки чому робочі

характеристики кожної бази прецедентів з часом й накопиченням досвіду безперервно поліпшуються.

Оскільки методологія CBR застосовувалася і показала гарні результати в предметних областях для класифікації, діагностики, прогнозування, планування і проектування, то її залучення в дослідженні різноманітних напрямів інформаційної безпеки, особливо при оцінці ризиків, виявлення вторгнень, аналізу стану мережевої безпеки та інших аспектів, дозволить прийняти зважене управлінське рішення.

Постановка задачі. Нехай в Центрі Інформаційної безпеки підприємства збираються дані з усіх доменів та проводиться їх аналіз. Збір даних відбувається з використанням електронної пошти та інших сервісів, шляхом отримання електронних листів від адміністраторів доменів безпеки, які містять заявку з відомостями про інцидент.

Інформація, яку необхідно надати домену у зворотній заявці має таку структуру: наслідки інциденту; можливий рівень збитків; служба реагування, до якої необхідно звернутись; дії з ліквідації наслідків; етапи розслідування інциденту; фактичний час обробки інциденту; дії для попередження інциденту; коментарі команди реагування Центру ІБ.

Реалізація поставленої задачі. Перший кроком у вирішенні поставленої задачі є розробка онтології – процесу формалізації області знань про інциденти ІБ за допомогою концептуальної схеми; визначення термінів предметної області та відносин між ними.

Етапи розробки онтології:

1. Визначення класів;
2. Організація ієрархії класів;
3. Визначення атрибутів та властивостей класів;
4. Визначення індивідів та призначення їх атрибутам та властивостям конкретних значень.

Для розробки онтології пропонується редактор Protege (версія: 3.4.) - відкритий редактор онтологій і фреймворк для побудови баз знань.

Опишемо процес створення онтології в Protege 3.4.

Отже, нам необхідно створити базу знань прецедентів, де одним прецедентом є дані про один інцидент інформаційної безпеки.

Для суперкласу owl: Thing створюємо три непересічні підкласи верхнього рівня (рис. 2.).

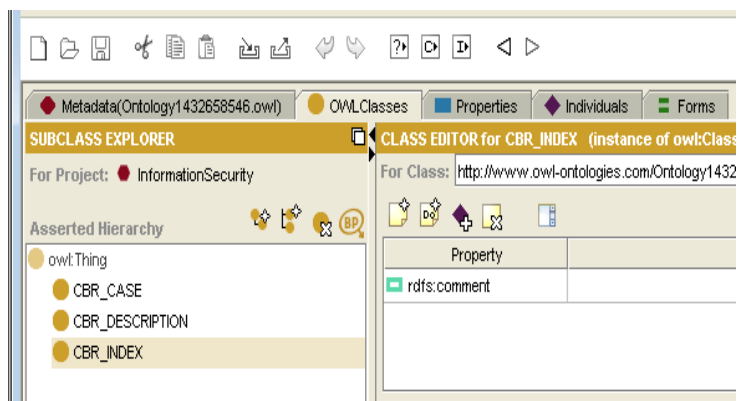


Рис. 2. Підкласи верхнього рівня

Запропонована структура необхідна для виконання завдання у програмному продукті jColibri. До підкласів верхнього рівня слід віднести:

- а) CBR_CASE - клас, що містить екземпляри прецедентів;
- б) CBR_DESCRIPTION – клас, що описує обмеження;
- в) CBR_INDEX - клас, який включає в себе параметри прецедентів.

На верхньому рівні концепти не перетинаються, тобто є непересічними класами.

Класи CBR_DESCRIPTION і CBR_CASE мають в якості підкласу нащадка - Інцидент_ІБ - два класи ідентичних один одному. Підклас Інцидент_ІБ класу CBR_CASE зберігає в собі самі прецеденти.

Для класу CBR_INDEX створено два підкласу-нащадка (рис. 3.):

- 1) Атрибути;
- 2) Рішення.

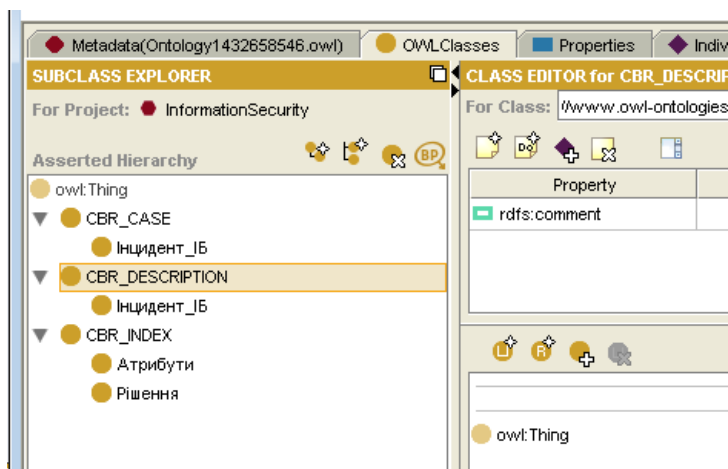


Рис.3. Підкласи класів верхнього рівня

Клас Атрибути містить підкласи, які відповідають параметрам та характеризують інцидент ІБ (рис. 5.):

- 1) а_Тип_інциденту;
- 2) б_Механізм_реалізації;
- 3) в_Група_підприємств;
- 4) г_Активи_під_загрозою;
- 5) д_Елементи_інформаційної_інфраструктури_під_загрозою;
- 6) е_Клас_інформації_під_загрозою;
- 7) ж_Порушена_властивість_інформації;
- 8) з_Джерело_загрози;
- 9) к_Кількість_джерел_загроз_ІБ;
- 10) л_Тип_джерела_загрози;
- 11) м_Категорія_персоналу_джерела_загрози.

Клас Рішення містить підкласи, що відповідають параметрам, які характеризують наслідки та дії з ліквідації наслідків інциденту ІБ (рис. 4.):

- 1) а_Наслідки;
- 2) б_Можливий_рівень_збитків;
- 3) в_Служба_реагування;
- 4) г_Дії_по_ліквідації_наслідків;
- 5) д_Етапи_розслідування_інциденту;

- 6) е_Фактичний_час_обробки_інциденту;
- 7) ж_Дії_для_попередження_інциденту.

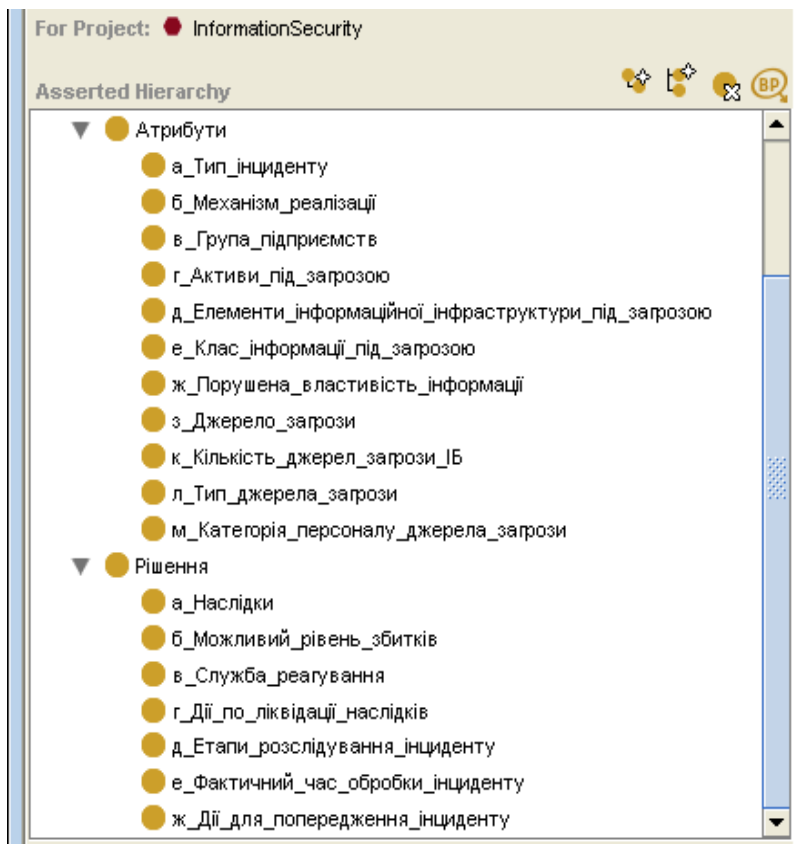


Рис. 4. Підкласи класів Атрибути та Рішення

Використовуючи вкладку Properties визначимо властивості, які матиме кожен індивід - прецедент. Властивостей стільки ж, скільки і класів у CBR_INDEX (рис. 5). Це параметри кожної конкретної ситуації-інциденту та її рішення.

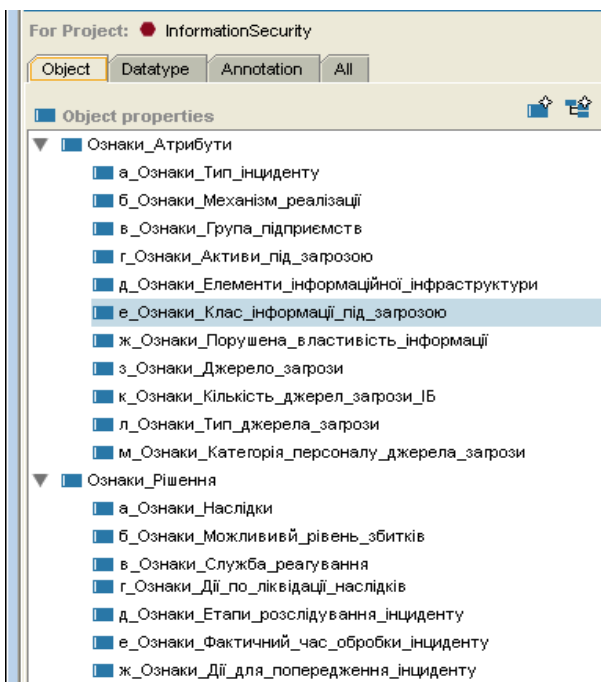


Рис. 5. Властивості індивідів - прецедентів

Створимо список можливих значень для кожного класу/властивості (рис. 6).

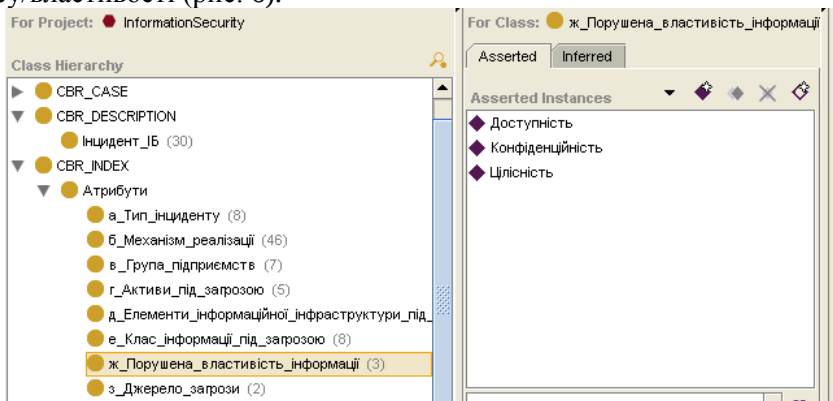


Рис. 6. Значення підкласу
«ж_Порушена_власивість_інформації»

На вкладці Individuals, для кожного підкласу класів Атрибути та Рішення з CBR_INDEX заповнюємо можливі значення для кожного класу/властивості.

Так, наприклад, клас

ж_Порушена_властивість_інформації може приймати такі властивості:

- 1) Цілісність;
- 2) Доступність;
- 3) Конфіденційність.

Перелік значень для кожного підкласу класів Атрибути та Рішення наведено в Таблиці 1.

Таблиця 1

Значення підкласів класів «Атрибути» та «Рішення»

№	Назва підкласу	Значення
Клас: Атрибути		
1	а_Тип_інциденту	DDos-атака, Phishing, Несанкціонований_доступ, Перевищення_повноважень, Шахрайство, Шпигунство, Недбалість_співробітників, Загрози_природного_походження
2	б_Механізм_реалізації	DDoS_атаки_на_DNS-сервери, HTTP-флуд, ICMP-флуд, UDP-флуд, SYN-флуд, Зараження_AC_вірусами, Ботнет, Malware, Масові_розсилки_електронних_листів, Масові_розсилки_особистих_повідомлень_в_межах_сервісу, Зараження_імітованих_IP-протоколів_вірусами_або_шкідливими_програмами, Фальсифікування_протоколів_маршрутизації, перехоплення_IP-протоколів_іншого_абонента, Підміна_даних_IP-протоколів_через_вразливості_протоколів_стеку_TCP/IP, НСД_до_сервісів_передачі_даних, Розвідка_IP-протоколів, Несанкційоване_копіювання_інформації, Підкуп_персоналу, Шантаж_персоналу, Фізичне_руйнування_ел-тів_інф.інфраструктури, Модифікація_технічної_інформації, НСД_неавторизованих_осіб,

№	Назва підкласу	Значення
		НСД авторизованих осіб, Крадіжка елементу інф. інфраструктури, Крадіжка носія інформації, Виведення з ладу інформаційно-телекомунікаційної системи, Втрата кінцевого пристрою користувача, Втрата носія інформації, Розголошення атрибутів розмежування доступу, Втрата атрибутів розмежування доступу (паролів, ключів шифрування), Викрадення атрибутів розмежування доступу, Ненавмисне пошкодження елементів інф. інфраструктури, Навмисне пошкодження елементів інф. інфраструктури, Помилки системного адміністратора у зміні конфігурації, Помилки адміністратора безпеки при призначенні прав доступу, Помилки розробників при розробці ПЗ, Злочинні дії персоналу, Помилкові дії персоналу, Відмова в роботі веб-серверу, Відмова в роботі XML-серверу, Відмова в роботі серверу баз даних, Виведення з ладу операційної системи, Помилки конфігурації, Помилки маршрутизації, Пожежа, Повінь, Землетрус, Техногенна аварія
3	в Група підприємств	Державні та комунальні структури, Промисловість і виробництво, Торгівля і послуги, Транспорт та зв'язок, Освіта та культура, Охорона здоров'я, Фінансові установи
4	г Активи під загрозою	Виробничі основні засоби, Невиробничі основні засоби, Фінансові активи, Об'єкти інтелектуальної власності, Товарно-матеріальні запаси
5	д Елементи інформаційної інфраструктури під загрозою	Апаратне забезпечення, Програмне забезпечення, Елементи локальної мережі, Елементи корпоративної мережі, Елементи зовнішньої мережі, Носії інформації, Інформація, Сервер, Системні ресурси, Обчислювальна система
6	е Клас інформації під загрозою	Державна таємниця, Комерційна таємниця, Конфіденційна інформація, Інформація внутрішнього обліку,

№	Назва підкласу	Значення
	грозою	Персональні дані клієнтів, Відкрита інформація, Персональні дані співробітників
7	ж_Порушен а_властивість інформації	Конфіденційність, Цілісність, Доступність
8	з_Джерело_з агрози	Зовнішній, Внутрішній
9	к_Кількість джерел_заг роз_ІБ	Один, Більше_одного
10	л_Тип_джер ела_загрози	Персонал підприємства, Зовнішнє природне середовище, Представники сторонніх організацій (конкуренти), Представники сторонніх організацій (партнери), Представники сторонніх організацій (посередники), Клієнти, Кримінальні структури, Хакер, Програмне забезпечення, Апаратно-програмні комплекси, Невідомо
11	м_Категорія_ персоналу_д жерела_заг рози	Адміністратор системи, Адміністратор безпеки, Персонал IT-відділу, Персонал служби ІБ, Керівники проміжних ланок, ТОП-менеджмент, Технічний персонал, Обслуговуючий персонал, Персонал функціонального відділу, Відсутня
Клас: Рішення		
1	а_Наслідки	Матеріальні збитки, Збитки репутації компанії, Порушення закону, Прості сервісів, Відмови сервісів, Порушення недоторканності приватного життя клієнтів, Крадіжка особистості, Крадіжка інтелектуальної власності, Загрози здоров'ю, Зниження акціонерної вартості, Судові процеси
2	б_Можливи й_рівень_зби тків	Збитки відсутні, Низький рівень, Середній рівень, Високий рівень, Неприпустимо високий рівень.
3	в_Служба_р еагування	Служба IT, Служба ІБ, Відділ кадрів, Юридична служба, Служба безпеки, Бізнес-менеджери, ТОП-менеджмент, Служба зв'язків з громадськістю, Правоохоронні органи, Стороння організація з Розслідування інцидентів ІБ, Провайдер послуг Інтернет
4	г_Дії_по_лік відації_наслі	Блокування атаки, Ресетрація DoS-атаки для подальшого аудиту,

№	Назва підкласу	Значення
	дків	Оповіщення співробітників про інцидент, Відновлення даних, Додати інформацію в антифішингові фільтри браузерів, Зміна параметрів конфігурації ПЗ компонент АС, Зміни конфігурації програмно-апаратних засобів РС, Зміна атрибутів доступу користувача, Встановити число «напіввідкритих» з'єднань, Підрахувати кількість підключень на 80 порт, Підрахувати кількість процесів Apache, Подивитися список IP-адрес, Провести аналіз пакетів за допомогою команди tcpdump, Скинути з'єднання на маршрутизаторі, Заміна пошкоджених ел-тів інф. Інфраструктури, Відновлення інформації з резервних копій, Подати заяву в міліцію про втрату, Подати заяву в міліцію про крадіжку, Подати заяву в міліцію про шахрайство, Ремонт пошкодженого обладнання, Заміна пошкодженого обладнання
5	д Етапи розслідування і інциденту	Звернення до правоохоронних органів, Звернення до сторонньої організації з Розслідування інциденті в ІБ, Повідомлення про інцидент до CERT-UA, Збір свідчень інциденту для паперових документів: зберігаєм оригінал з записами про особу, яка знайшла документ, Збір свідчень інциденту для паперових документів: зберігаєм оригінал з записами про місце, де документ був виявлений, Збір свідчень інциденту для паперових документів: зберігаємо оригінал з записами про час, коли документ був виявлений, Збір свідчень інциденту для паперових документів: зберігаєм оригінал з записами про особу, що засвідчила виявлення, Збір свідчень інциденту для електронних документів: копія н осія інформації для забезпечення доступності. Збір свідчень інциденту для електронних документів: копія ін формаші на жорстких дисках для забезпечення доступності. Виявлення фішингового домену, Відновлення хронометражу подій, Пошук доказів на носіях інформації, Порушення кримінальної справи,

№	Назва підкласу	Значення
		Подача позову проти порушника, Адміністративний вплив, Пошук замовника атаки, Пошук виконавця атаки, Визначення конкретного джерела: хакер чи клієнт (банківський сектор), Отримати юридичний супровід розслідувань в правоохоронних органах, Результат: Адміністративні стягнення Результат: Догода працівнику Надати лог-файли web-сервера, Надати лог-файли ядра самого комп'ютера, Надати лог-файли брандмауера Надати списки виявлених IP-адрес
6	е Фактичний час обробки інциденту	до 24-х годин, від 1 до 7 діб, від 1 до чотирьох тижнів, від 1 місяця до 6 місяців, більше 6 місяців
7	ж Дії для попередження інциденту	Розробка системи захисту інформації, Архівация даних, Розмежування доступу, Відслідковувати правові рішення в області комп'ютерних злочинів, Встановлення режиму інформаційної безпеки, Створення Helpdesk, Налаштувати систему журналювання в ІС, Налаштувати процедуру реагування на інцидент ІБ, Посилення захисту паролів, Посилення захисту ключів ЕЦП, Вдосконалення системи криптографічного захисту інформації, Вдосконалення системи технічного захисту інформації на програмному рівні, Вдосконалення системи технічного захисту інформації на апаратному рівні, Вдосконалення системи технічного захисту інформації на мережевому рівні, Оцінка та переоцінка ризиків ІБ, Підготовка переліку захисних заходів для мінімізації виявлених

№	Назва підкласу	Значення
		х ризиків, Актуалізація політик, регламентів та правил ІБ, Навчання персоналу основам та правилам ІБ, Налаштування оповіщень в консолі антивірусу, Налаштування оповіщень в консолі IDS системи, Налаштування оповіщень в консолі DLP системи Використання браузерів, що попереджають про загрозу фішингу, Ускладнення процедури авторизації, Установка системи виявлення DoS-атак на мережних магістральних каналах, Відключити відповіді на запити ICMP_ECHO, Збільшити одночасну кількість максимальних підключень до бази даних сервера, Встановити перед Web-сервером Apache продуктивний Nginx для кешування запитів, Встановити обмеження на кількість з'єднань до DNS-сервера, Відключити відсилання UDP-пакетів на різні UDP-сервіси, Відключення черги напіввідкритих TCP-з'єднань, Включення механізму TCP_syncookies, Обмеження максимального числа «напіввідкритих» з'єднань з одного IP до конкретного порту, Налаштування системи аналізу трафіку, яка допоможе вчасно дізнатися про наближення DoS-атаки, Підготовка усіх серверів, які мають доступ в зовнішню мережу до віддаленого аварійного перезавантаження, Забезпечення другого мережевого інтерфейсу, через який по ssh-з'єднанню можна швидко отримати доступ до сервера, Підтримка актуальності програмного забезпечення, Захист всіх мережних сервісів брандмауером, Своєчасна установка оновлень, Користуватись режимом автоматичних оновлень, Використовувати ліцензовані копії ОС та ПЗ, Обмежити фізичний доступ до комп'ютера сторонніх осіб, Робити резервне копіювання важливої інформації, Установка пароля на завантаження ОС, Використання засобів шифрування жорсткого диска, Застосування біометричних засобів контролю, Ознайомлення персоналу з правилами техніки безпеки

№	Назва підкласу	Значення
		Використання <u>SYN cookie</u> , Використання мережевого протоколу SCTP замість TCP.

Джерело: розроблено авторами самостійно

Кожна властивість конкретного прецеденту може приймати одне або більше значень, які задаються для підкласів. Тобто, властивість певного прецеденту ж Порушена_властивість_інформації може приймати значення «Цілісність», або «Доступність», або «Конфіденційність», або «Цілісність» та «Доступність», тощо. Тому задані попередньо властивості необхідно зв'язати із підкласами з CBR_INDEX. Для цього використовуємо логічний оператор $\exists$, або *some*, який означає, що властивість приймає значення принаймні одного елемента області визначення класу. Результати прийнятих значень представлені рис. 7.

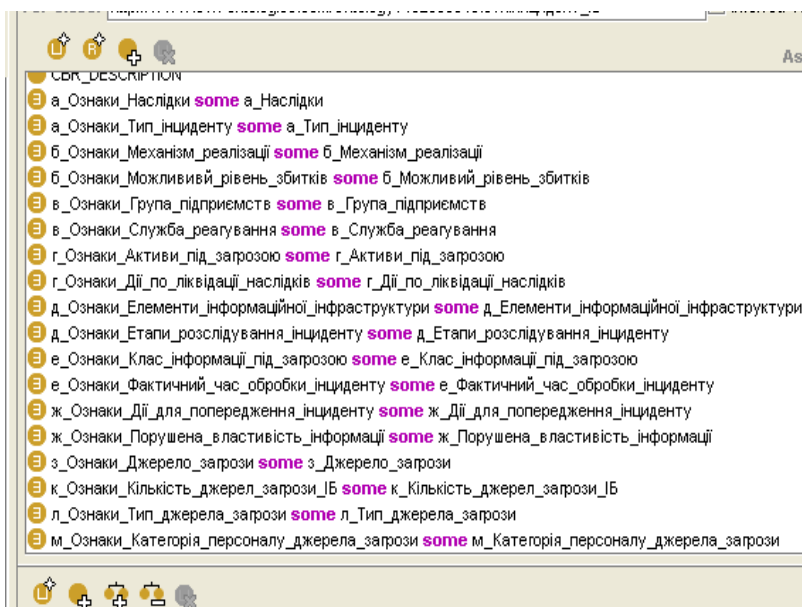


Рис. 7. Зв'язка властивостей із підкласами з CBR_INDEX за допомогою оператора *some*

Після представлення задамо Individuals для підкласу Інцидент_ІБ класу CBR_CASE, який містить екземпляри прецедентів. Тобто створимо базу прецедентів. Для кожного прецеденту визначимо значення окремої властивості (рис. 8).

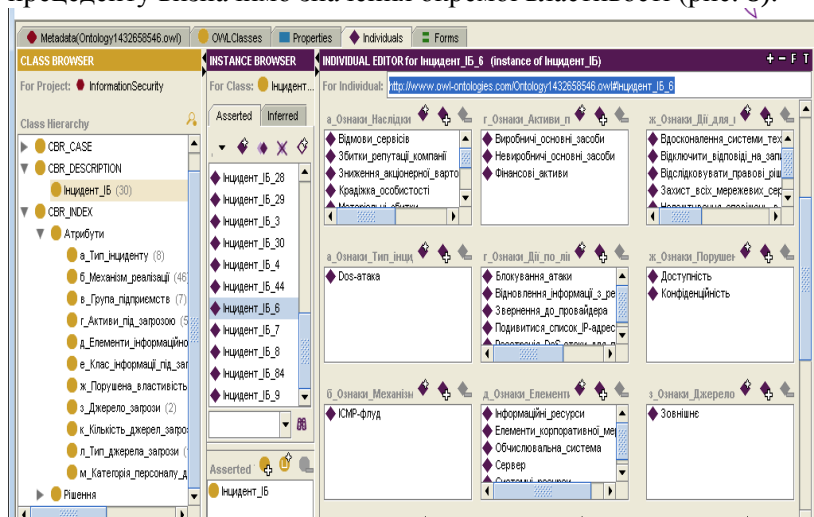


Рис. 8. Визначення властивостей для прецеденту «Інцидент_ІБ_6»

В результаті, нами була створена база прецедентів із 30 екземплярів. На цьому робота з Protégé завершена. Маємо owl-файл онтології. Подальше використання онтології передбачає застосування інструментарію jColibri.

Міркування з прецедентами будемо використовувати для пошуку найбільш схожих прецедентів із заданим інцидентом у створеній базі прецедентів.

Ступінь близькості інциденту та прецеденту визначається на основі ступеня близькості відповідних параметрів, ознак ситуацій. Кожному параметру присвоюється ваговий коефіцієнт, який відображає його відносну важливість.

Для визначення ступеня близькості інциденту та прецеденту за всіма ознаками використовуємо наступну формулу:

$$sim(i, p) = \frac{\sum_{j=1}^n w_j * sim(e_{ij}, e_{pj})}{\sum_{j=1}^n w_j}, \quad (1)$$

де sim – метрика подібності;

i, p – інцидент і прецедент відповідно;

w_j – ваговий коефіцієнт j -ої ознаки;

e_{ij}, e_{pj} – значення ознаки e_j для інциденту та прецеденту відповідно.

Вибір метрики подібності ознак (1) є дуже важливим завданням, оскільки пошук схожих ситуацій значно залежить від цього вибору. В дослідженні була обрана метрика EQUAL, яка означає рівність ознак інциденту та прецеденту.

Ваги слугують для балансування важливості і впливовості параметра прецеденту. Значення кожного вагового коефіцієнта задаємо в межах від 0 до 1: $w_j \in [0; 1]$.

Для створення індивідуальної CBR-системи перейдемо до програмного продукту jColibri. jColibri - об'єктно-орієнтована платформа мовою Java для створення CBR-систем, в тому числі, базуючись на онтологіях з описовою логікою. В даному дослідженні для створення CBR-системи була використана версія 1.1.

Після створення нової CBR-системи «InformationSecurityIncidents» з розширенням Description Logic Extension (використання описової логіки) відбувається налаштування структури онтології та кожного параметра прецеденту (рис. 9).

Як бачимо, в якості основних параметрів прецеденту обрано підкласи класу Атрибути зі створеної попередньо онтології. Саме ці характеристики інциденту будуть вхідним даними для нашої CBR-системи.

На основі інструментарію jColibri був згенерований клас мовою Java. Після створення всіх необхідних java-методів, було отримано успішно функціонуючий Java-додаток, який має вигляд форми для введення параметрів інциденту.

Після проведення тестування створеної системи шляхом введення параметрів існуючого в базі знань прецеденту – Інцидент_ІБ_21 отримаємо результат – тестування пройшло успішно – значення міри подібності прецеденту із самим собою становить 1 або 100-відсоткова подібність.

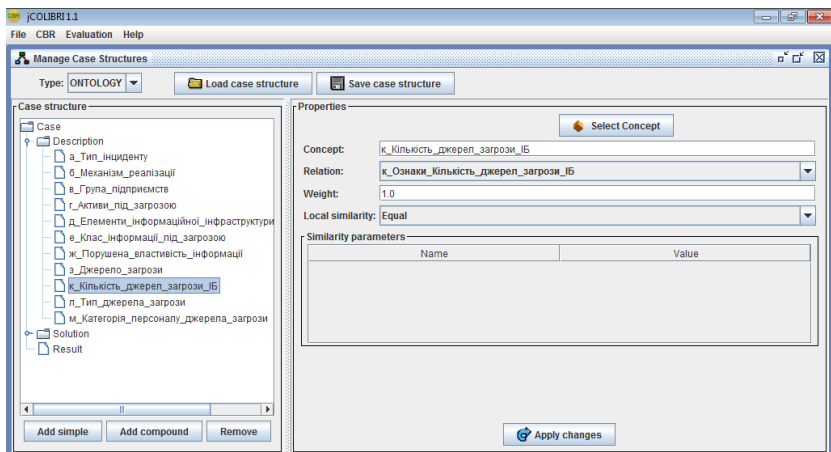


Рис .9. Налаштування параметрів прецеденту

В якості прикладу виявимо найбільш схожі прецеденти для конкретного інциденту, параметри якого наведемо в Таблиці 2.

Таблиця 2

Заявка на обробку інциденту ІБ від домену безпеки

№	Поле	Дані
1.	Тип інциденту	Dos-атака
2.	Механізм реалізації	SYN-флуд
3.	Активи під загрозою	Фінансові активи
4.	Елементи інформаційної інфраструктури під загрозою	Системні ресурси
5.	Клас інформації під загрозою	Витік інформації відсутній
6.	Порушена властивість інформації	Доступність
7.	Джерело загрози	Зовнішнє
8.	Кількість джерел загроз	Більше одного

№	Поле	Дані
9.	Тип джерела загрози	Хакер
10.	Категорія персоналу – джерела загрози	Відсутня
11.	Дата та час виявлення інциденту	25.05.2015, 15:34
12.	Місце виявлення інциденту	Сервер
13.	Примітки	Проблеми з встановленням зв'язку, затримки встановлення зв'язку

У темі листа зазначено назву домену та групу підприємств, до якої воно відноситься – «Торгівля і послуги».

В Центрі ІБ дані отриманої заявки вводяться в форму прецеденту, приклад якої представлено на Рис. 10 .

Requested parameters		
a_Тип_інциденту	Dos-атака	1.0
б_Механізм_реалізації	SYN-флуд	1.0
в_Група_підприємств	Торгівля_і_послуги	1.0
г_Активи_під_загрозою	Фінансові_активи	1.0
д_Елементи_інформаційної_інфраструктури_під_загрозою	Системні_ресурси	1.0
е_Клас_інформації_під_загрозою	Витік_інформації_відсутній	1.0
ж_Порушена_властивість_інформації	Доступність	1.0
з_Джерело_загрози	Зовнішнє	1.0
к_Кількість_джерел_загрози_ІБ	Більше_одного	1.0
л_Тип_джерела_загрози	Хакер	1.0
м_Категорія_персоналу_джерела_загрози	Відсутня	1.0

Рис. 10. Введення параметрів інциденту ІБ в форму CBR-системи

Результатом роботи CBR-системи є звіт, в якому вказуються значення мір подібностей даного інциденту з кожним прецедентом (рис. 11).

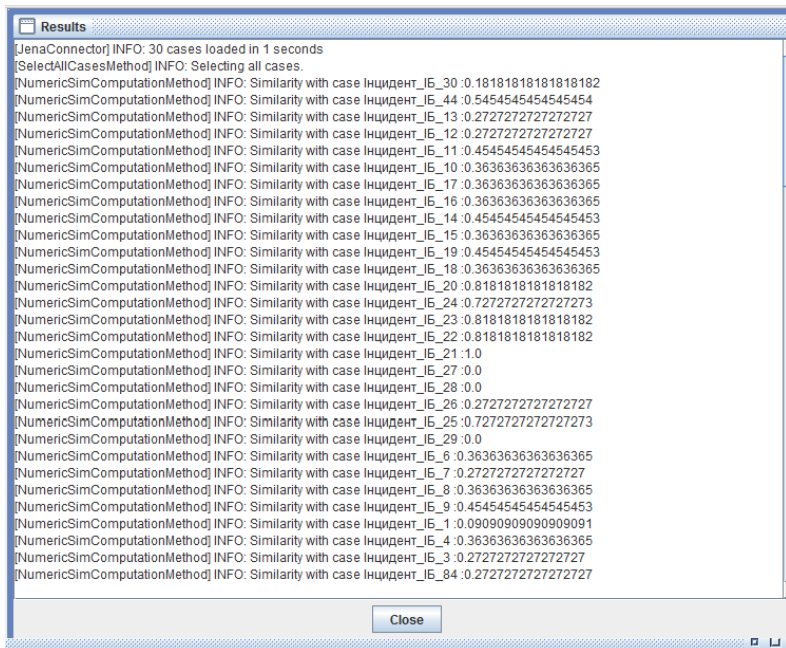


Рис. 11. Звіт з проведення тестового запиту

Як бачимо із згенерованого звіту, найбільше значення міри подібності Similarity with case: 0,818182 інцидент має з прецедентами: Інцидент_ІБ_4, Інцидент_ІБ_8, Інцидент_ІБ_9.

Команда реагування Центру ІБ звертається до бази знань і аналізує параметри зазначених інцидентів, які відносяться до класу Рішення.

Результат аналізу – лист-відповідь від команди реагування Центру ІБ, який містить рекомендації та коментарі за даним інцидентом. Приклад відповіді наведено в Таблиці 3.

В домені безпеки рекомендації Центру ІБ аналізуються системним адміністратором, приймаються рішення і здійснюються відповідні заходи для ліквідації наслідків інциденту. Дані про інцидент заносяться до Журналу інцидентів ІБ. В домені безпеки рекомендації Центру ІБ аналізуються системним адміністратором, приймаються рішення і здійснюються відповідні заходи для ліквідації наслідків інциденту. Дані про інцидент заносяться до Журналу

інцидентів ІБ. Після закриття інциденту до Центру ІБ надсилається звіт з інформацією про інцидент, способи і результати усунення наслідків.

Таблиця 3

Відповідь від Центру ІБ

Тип інциденту: Dos-атака		
Механізм реалізації: SYN-флуд		
№	Поле	Дані
1.	Наслідки	Простої сервісів, Відмови сервісів, Матеріальні збитки
2.	Можливий рівень збитків	Низький - Середній
3.	Служба реагування	Системний адміністратор, Служба ІТ, Служба ІБ
4.	Дії по ліквідації наслідків	1. Встановити число напіввідкритих з'єднань 2. Збільшити чергу напіввідкритих з'єднань 3. Зменшити час очікування з'єднань 4. Додати обмеження чиста SYN-пакетів на 1 часу
5.	Етапи розслідування інциденту	1.Встановлення джерела атаки 2. Визначення виконавця атаки 3.Визначення замовника атаки 4. Надання лог-файлів сервера 5. Надання списку шкідливих IP-адрес 6. Звернення до правоохоронних органів
6.	Фактичний час обробки інциденту	Від 1 до 7 діб
7.	Дії для попередження інциденту	1. Використання <u>SYN cookie</u> 2. Обмеження кількості запитів на нові підключення від конкретного джерела за певний проміжок часу 3. Використання мережевого протоколу SCTP замість TCP
8.	Коментарі	Виявлення атаки: команда netstat надає список напіввідкритих з'єднань

Висновки. Методологія CBR особливо важлива для забезпечення прийняття рішень в екстремальних ситуаціях, які характеризуються гострим дефіцитом часу і швидко мінливою обстановкою, яка характерна для ситуацій загрози інформаційній безпеці. Частина завдань екстремальних ситуацій може виявитися вже раніше розв'язаною, а наявні рішення можуть бути основою для оперативного отримання варіантів ситуаційного управління на даний момент часу. Повторне використання інформації та досвіду дозволить зменшити час, який витрачається на вирішення нової проблеми, поліпшити якість прийнятого рішення.

Таким чином, ілюстрація реалізації моделі ситуаційного управління у Центрі інформаційної безпеки й наведений контрольний приклад взаємодії домену безпеки та Центру з вирішенню ситуації інциденту дозволив звернути увагу на такі проблеми: необхідність роботи досвідчених експертів з управління інцидентами ІБ в доменах безпеки; ризик прийняття помилкового рішення при управлінні інцидентом ІБ; відсутність централізованого джерела статистики за інцидентами ІБ.

Список використаних джерел:

1. Шенк Р. К. Обработка концептуальной информации : пер. с англ. / Роджер К. Шенк ; Пер. Г.В. Сенин ; Под ред. В.М. Брябрин . – Москва : Энергия, 1980 . – 361 с.
2. Имамвердиев, Я. Н. Модель ситуационного управления информационной безопасностью электронного правительства / Я. Н. Имамвердиев // Информационные технологии. - 2014. - № 8.
3. Бегун А.В. Інформаційна парадигма безпеки економічної системи/А.В. Бегун// Моделювання та інформаційні системи в економіці:[зб. наук. праць]/відп. ред. Галіцин ВК–К.: КНЕУ.– 2011.–Вип. 78.–с. 182-190
4. Бегун А.В., Ігнатова Ю.В. Моделювання проактивного визначення ddos-атаки/ А.В. Бегун, Ю.В. Ігнатова// Моделювання та інформаційні системи в економіці : Зб. наук. праць – К. : КНЕУ, 2015. – Вип. 91.– с. 262-274