DOI: 10.18372/2410-7840.19.11681
УДК 004.056.53

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНОЇ ОНТОЛОГІЇ ДЛЯ ПРОЕКТУВАННЯ ТА АНАЛІЗУ КСЗІ

Олександр Архипов, Олег Козленко

У статті пропонується варіант онтологічної структури як специфічної формально-логічної схеми, що дозволяє накопичувати та впорядкувати відомості про типові загрози інформації, заходи та засоби з їх нейтралізації, аналізувати ефективність можливих варіантів побудови системи захисту інформації. Формування онтології виконується з орієнтацією на найбільш поширені варіанти сценаріїв ураження інформації та на типові вразливості організації, обумовлені характерним для неї станом та рівнем культури інформаційної безпеки. Дана онтологічна структура може бути використана для обчислення значень інформаційних ризиків для типових сценаріїв ураження інформації, формування базової системи захисту інформації та визначення узагальненої оцінки захищеності організації у інформаційній сфері.
Ключові слова: *онтологічна структура, оцінювання ризику, сценарії витоку інформації, культура інформаційної безпеки, онтограф, загрози інформації, рівень культури інформаційної безпеки.*

Вступ. Забезпечення надійного захисту інформації потребує значних коштів. Тому перед впровадженням захисних заходів потрібно впевнитися у їх доцільності. Зокрема, збереження конфіденційних даних для багатьох компаній є одним з головних пріоритетів у веденні успішного бізнесу, а інформація про конкурентів може допомогти побудувати свій бізнес-план таким чином, щоб випередити їх на декілька кроків. В загальному випадку витік даних може призвести не тільки до значних фінансових втрат, але й до повного розпаду підприємства.

Для захисту організації від витоків інформації або інших інформаційних загроз необхідно провести повний аналіз захищеності її інформаційних систем. Він має спиратися на різноманітні методи та заходи, зокрема, дослідження сценаріїв витоку інформації, інше. Крім того, треба враховувати адміністративні аспекти захисту інформації, такі як інформованість персоналу про загрози інформації. Тому для оцінювання, наприклад, значення ризику втрат від витоку інформації потрібно враховувати дуже багато факторів, їх взаємозв'язки та взаємозалежність. В цьому випадку надзвичайно важливою стає можливість застосування певної формальної структури, що містить детальний опис сукупності визначених факторів, сценарії їх взаємодії і т.п., що буде значно спрощувати розуміння та автоматизацію аналізу ризиків, проведення відповідних розрахунків для їх подальшого використання. Окрім того, безпека організації залежить не тільки від стану технічних активів її інформаційної системи. Звичайні помилки персоналу системи, нерозуміння ним наслідків інцидентів безпеки, невчасна та неадекватна реакції на них теж відіграють важливу роль. Дана стаття фокусується на застосуванні інформаційної онтології як системно-структурного засобу, що може використовуватися для побудови та аналізу комплексної системи захисту інформації (КСЗІ) в організації, визначення оцінки загального стану безпеки інформації в організації та автоматизації процесу отримання цієї оцінки.

Теоретичні аспекти побудови онтології предметної області. Процес побудови 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, що базується на понятті «онтології». Серед фахівців, що займаються проблемами комп'ютерної лінгвістики, найбільш усталеним (класичним) вважається визначення онтології, дане Т. Грубером: «Онтологія - це специфікація концептуалізації» [1]. Існує ще ряд розширених визначень Т. Грубера, 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 [2];

– 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 [2].

Якщо підходити до визначенням поняття «онтологія» з формальним позицій, то згідно [3] під

комп'ютерною онтологією предметної області (Пдо) розуміється трійка: $O =< X, R, F >$, де $X = \{x_1, x_2, \dots, x_i, \dots, x_n\}$, $i = \overline{1,n}$, $n = Card\ X$ - скінченна множина концептів (понять) заданої Пдо; $R = \{r_1, r_2, \dots, r_k, \dots, r_m\}$, $R = x_1 * x_2 * \dots * x_n$, $k = \overline{1,m}$, $n = Card\ R$ - скінченна множина семантично значущих відносин між концептами Пдо. У загальному випадку відносини ділять на загальнозначущі (з яких виділяють, як правило, відносини часткового порядку) і конкретні відносини заданої Пдо. $F = X * R$ - скінченна множина функцій інтерпретації, заданих на концептах або відносинах. Окремим випадком завдання множини функцій інтерпретації *F* є глосарій, складений для множини понять X. Визначення поняття X_i в загальному випадку включає підмножину понять $\{x_{i-1}\}$, через які визначається X_i, відношення R_k, що зв'язує X_i з $\{x_{i-1}\}$, і множину атрибутів (ознак), властивих X_i.

Хоча вищезазначені множини і складають онтологію, найбільш зручно зображати онтологію у виді онтографу. Онтограф - це односпрямований орієнтований граф, вершинами якого є поняття предметної області, а дугами - зв'язки між ними; в одну вершину онтографу може входити і виходити кілька дуг.

У простому випадку методика проектування онтології Пдо включає три етапи проектування:

1. Попередній аналіз предметної області;
2. Побудова вручну ондографа Пдо;
3. Графічне (візуальне) проектування ондографа Пдо.

Найбільш важливим вважається перший етап проектування онтології Пдо (Попередній аналіз предметної області), бо саме на цьому етапі визначаються основні терміни і відношення між ними. В ході проектування онтології для побудови КСЗІ організації перш за все потрібно провести дослідження можливих сценаріїв втрат інформації для визначення необхідних елементів її захисту та аналіз адміністративного аспекту захисту інформації.

Сценарії витоку інформації. Аналіз інформаційних систем є складним процесом і включає в себе багато інших операцій. Однією із складових аналізу інформаційних систем є визначення елементів КСЗІ. Для формування елементів захисту організації від витоку інформації потрібно визначити та дослідити можливі загрози щодо інформації та відповідні необхідні дії захисту. Згідно [4] дії, що призводять до реалізації потенційних небезпек, які ведуть до ураження інформаційних ресурсів і через те мають потенційно можливий несприятливий вплив на активи організації, називаються загрозами, а спроба реалізації загрози називається атакою. Результати реалізації загрози можуть впливати на інформацію як безпосередньо, так і опосередковано. 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 (помилки персоналу або дії зловмисника), які в свою чергу можуть бути випадковими або навмисними. З точки зору захищеності інформація має три основні властивості: конфіденційність, цілісність і доступність, а загрози, порушення яких призводить до втрати інформацією будь-якої з вищезазначених властивостей, відповідно – загрозами конфіденційності, цілісності та доступності інформації.

Як зазначено у [4], 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, методи і заходи протидії загрозам якої керовані і безпосередньо залежать від розробників СЗІ. Друга група містить загрози, які безпосередньо залежать від технічних засобів інформаційної інфраструктури організації і їх властивостей, що сприяють утворенню каналів реалізації потенційних загроз захищеності інформації. Третя група складається із загроз, які абсолютно не прогнозуються і тому заходи для їх запобігання повинні застосовуватися до всіх елементів технічної інфраструктури підприємства чи організації.

Перша група загроз також включає в себе адміністративні загрози, такі як необізнаність персоналу про загрози для системи та інше, що у свій час може призвести до інцидентів витоку інформації через навмисні або ненавмисні дії.

Одними з таких інцидентів, наприклад, може бути промислове шпигунство та недобросовісність працівників. Потенціальними жертвами промислового шпигунства зазвичай виступають підприємства, що володіють або створюють певну інтелектуальну власність і можуть втратити конкурентну перевагу через втрату конфіденційної інформації.

Причиною витоку інформації можуть бути також просто недобросовісні працівники, що не дотримуються загальноприйнятих вимог та етичних правил: компанія будь-коли може постраждати від примітивного шахрайства або через ігнорування її працівниками політики безпеки (наприклад, ненавмисне зараження вірусом, перенесеним гральною програмою, корпоративної системи).

Зазвичай випадки, пов'язані з реалізацією інцидентів щодо витоку інформації, не підлягають розголошенню, аби не зашкодити репутації компанії. Тому надзвичайно цікаві щорічні огляди американської компанії Verizon [5, 6], присвячені дослідженню інцидентів в сфері інформаційної безпеки, зокрема розслідуванню випадків витоку даних. Verizon надає одне з найбільш розгорнутих зібрань статистичних відомостей та аналітичних висновків саме щодо витоку даних. Достовірність і точність відомостей обумовлюється тим, що дослідження базується на вибірці обсягом понад 100000 інцидентів [5] і охоплює понад 70 організацій більш ніж у 60 країнах, в тому числі й в Україні. Багаторічні дослідження компанія Verizon довели доцільність поділу інцидентів витоку даних на дев'ять базових 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 [5, 6]. Розподіл випадків розголошення даних у 2016 році [5] представлений на рисунку 1.

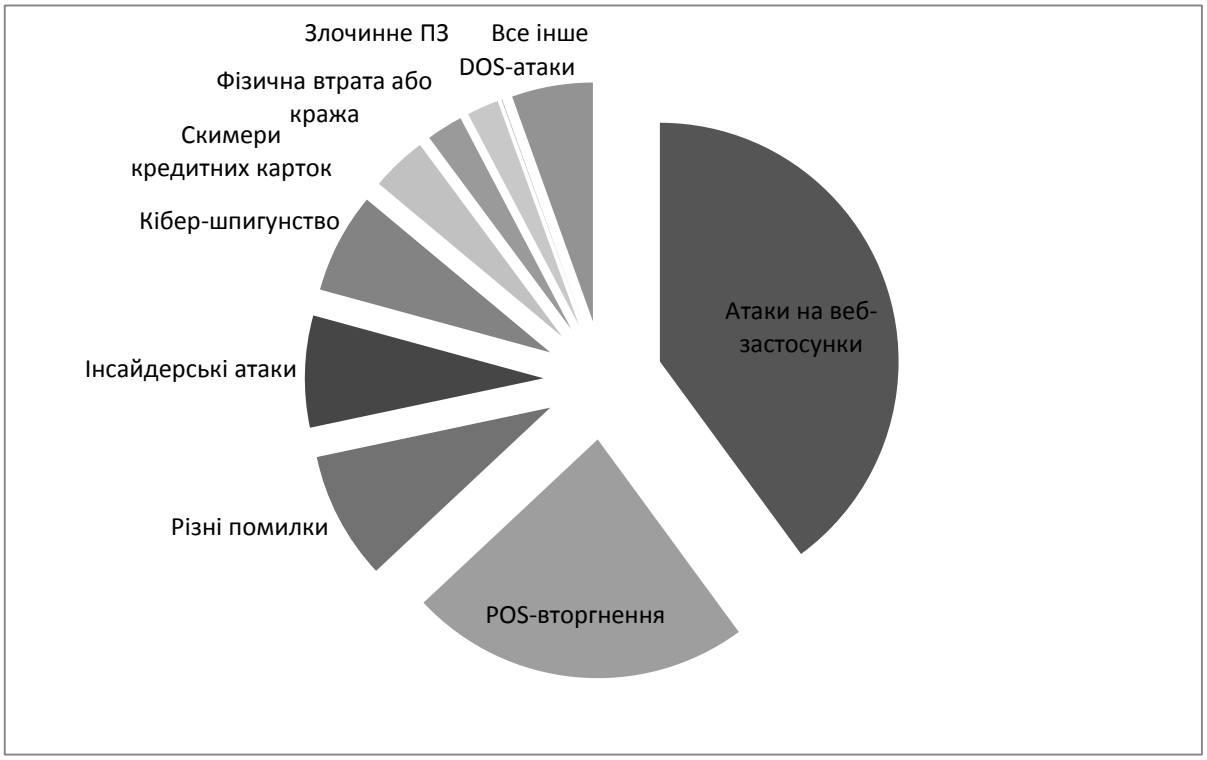

Рис. 1. Частота інцидентів з підтвердженим розголошенням даних

Для побудови онтології для аналізу комплексних систем захисту інформації нам необхідно розглянути кожний з цих сценаріїв окремо:

– Сценарій «Вторгнення в точки продажу» включає в себе атаки на середовища, де проводяться роздрібні торгові операції.

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

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

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

– В сценарій «Скимери платіжних карток» входять пристрої, фізично встановлені у місця зчитування даних з магнітних стрічок платіжних карток, метою яких є збір та підробка даних та незаконне втручання у платіжні операції.

– До сценарію «Фізична крадіжка або втрата» належать випадки крадіжки або загублення через неуважність фізичних носіїв інформації.

– В сценарій «Різні помилки» входять випадки ненавмисного компрометування атрибутів безпеки інформаційних активів, що не підходять під інші названі сценарії.

– Будь-яка атака, спрямована на порушення доступності мережі або системи належить до сценарію «DOS-атак». Як правило, такі інциденти в результаті не порушують конфіденційність інформації.

– Сценарій «Інсайдерських атак» охоплює всі інциденти, які сталися через те, що внутрішні працівники або довірені особи зловживали своїми правами чи свідомо недбало виконували свої обов'язки.

У звіті про витоки даних за 2016 рік компанія Verizon виділила загрози для кожного з вищезазначених сценаріїв, що дає змогу, спираючись на фактори, які Verizon виділила у звіті про витоки інформації за 2013 рік [7], визначити множину необхідних мір захисту, до складу яких входять:

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

– Відсутність непотрібного ПЗ, облікових записів, портів та ін. – система немає ПЗ, облікових записів, відкритих портів та ін., що не використовується.

– Оновлення та патчі – постійне 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 вебзастосунків 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.

– Паролі 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 Net Flow – облік мережевого трафіку.

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

– Акаунт-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.

Деякі міри захисту можливо об'єднати у більш узагальнені комплекси, визначені табл. 1.

Таблиця 1

Об'єднання мір захисту у більш узагальнені визначення

Узагальнене визначення	Міри захисту
Конфігурація	– Відсутність непотрібного ПЗ, облікових записів, портів – Оновлення та патчі – Цілісність системних файлів
Захист від шкідливого ПЗ	– Антивірусні програми – Оновлення захисних програм – DEP, ASLR ,EMET
Безпека розробок	– Тестування веб-застосунків – Закритість матеріалів для розробленого ПЗ
Обізнаність співробітників щодо вимог безпеки	– Тренінги по ІБ для співробітників – Перевірка працівників
Паролі	– Складні паролі – Паролі за замовчуванням
Управління акаунтами	– Акаунт-менеджмент – Централізована автентифікація – Моніторинг входів
Відповіді на інциденти	– Робота з інцидентами – Ролі при інцидентах

Культура інформаційної безпеки. Як зазначалося, не всі загрози безпосередньо залежать від технічних особливостей систем. Небезпеку також становить людський фактор, який не завжди обумовлюється нестачею або недосконалістю засобів захисту, але завжди пов'язаний з недотриманням вимог політики безпеки (ПБ) [8].

Дослідження людських чинників в області інформаційної безпеки привертає все більше увагу через те, що вони мають значний вплив на інформаційну безпеку в цілому і окремо на інсайдерську її складову. Згідно з результатами опитування, наведеними у [8, 9], більшість співробітників впевнені, що відповідальність за цілісність інформаційних активів лежить на співробітниках інформаційної безпеки, головним завданням яких є усунення помилок і інцидентів. Але, як і раніше, організації страждають від випадкових або навмисних помилок співробітників, незважаючи на наявність політики безпеки і необхідних технологій. Як зазначається у [9], є два можливих вирішення питання про недотримання вимог:

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

– Формування високого рівня культури інформаційної безпеки. Варіант досить довгостроковий у виконанні, але має тривалий ефект у разі успіху.

Важливо зазначити, що існує багато визначень терміну культури інформаційної безпеки (КІБ). Узагальнюючи більшість з них, можна сказати, що КІБ є набором цінностей, людських переконань, думок і моделей поведінки, які забезпечують певний ступінь відповідності вимогам ІБ в організації [8]. КІБ завжди позитивно або негативно впливає на організацію і завжди має місце. Як зазначено у [9], є фактори, які впливають на вибір поведінки працівником, а саме на нормативні переконання і встановлені норми поведінки. Нові працівники, які знаходяться в процесі адаптації до норм трудового колективу, керуються встановленими нормами поведінки з поступовим переходом до стандартної поведінки в трудовому колективі [8, 9, 10]. Таким чином, організаційна культура регулює діяльність працівників. Працівник приймає основи коректної поведінки в процесі соціалізації і це допомагає співробітнику прийняти встановлені закономірності поведінки і стандарти організації (незалежно від їх відповідності вимогам ІБ). Сам процес формування культури інформаційної безпеки [8] зображено на рис. 2. Згідно [8], КІБ визначається показниками «Персонал» 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». Ці показники будемо використовувати для подальшого аналізу і побудови досліджуваної структури.

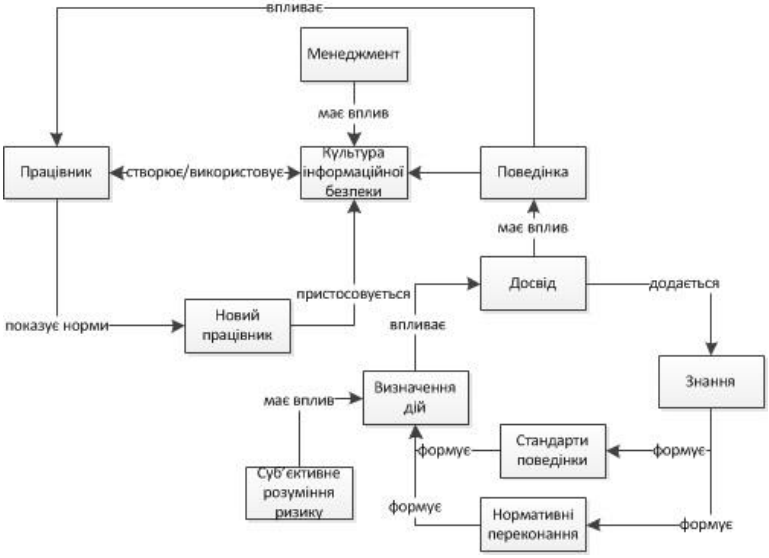

Рис. 2. Процес формування культури інформаційної безпеки

Побудова онтології предметної області. Побудуємо онтологічну структуру для аналізу КСЗІ, беручи за основу матеріали по вищезазначеним сценаріям з витоку інформації та рівню культури ІБ, спираючись на наведену вище методику побудови онтології. На першому етапі «Попередній аналіз предметної області» визначимо склад множин X та R. Множина понять X буде мати вигляд: {Центр безпеки, Конфіденційні дані, Політика безпеки, КІБ, Захист від витоку інформації, Персонал, Керівництво, Атаки на веб-застосунки, DoS-атаки, Інсайдерські атаки, Різні помилки, Фізична крадіжка або втрата, Скримери платіжних карток, Кібер-шпигунство, Злочинне ПЗ, POS-вторгнення, Управлінська готовність, Координованість, Співпраця з відділом ІБ, Співпраця з менеджментом, Кадрова безпека, Міра прийняття КБ, Захист від шкідливого ПЗ, Фільтрування трафіку, Журнал подій, Протокол Net Flow, Подвійна автентифікація, Контроль адміністраторів, Відокремлення серверів, Паролі, Інвентаризація ПЗ, Чорні та білі IP списки, Конфігурація, Обізнаність співробітників, Сегментація мережі, Оновлення та патчі, Відео спостереження, Перевірка те-

рміналів, Попередження користувачів, Ефективний дизайн, Резервне копіювання, Шифрування, DLP-система, Відсутність конфіденційних даних у відкритому тексті, Журнал подій, Управління акаунтами, Відповіді на інциденти, Безпека розробки }.Множина відношень *R* складається з відношень: {Ціле-частина, Визначає, Використовує}.

Наступним етапом є "Побудова вручну ондографа Пдо". Для цього виконуємо ранжування списку термінів по узагальненому відношенню «вище-нижче»:

– Центр безпеки.

– Конфіденційні дані, Політика безпеки.

– Захист від витоку інформації, КІБ.

– Атаки на веб-застосунки, DoS – атаки, Інсайдерські атаки, Різні помилки, Фізична крадіжка або втрата, Скримери платіжних карток, Кібершпигунство, Злочинне ПЗ, POS вторгнення, Управлінська готовність, Координованість, Персонал, Керівництво.

– 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 адміністраторів, Відокремлення серверів, Паролі, Інвентарізація ПЗ, Чорні та білі IP списки, Конфігурація, Подвійна автентифікація, Обізнаність співробітників, Сегментація мережі, Інвентарізація ПЗ, Оновлення та патчі, Відео спостереження, Перевірка терміналів, Попередження користувачів, Ефективний дизайн, Резервне копіювання, Шифрування, DLP-Система, Журнал подій, Управління акаунтами, Відсутність конфіденційних даних у відкритому тексті, Відповіді на інциденти, Безпека розробки.

Наступним та останнім етапом є «Графічне (візуальне) проектування ондографа Пдо» результат якого - це остаточне представлення структури онтології, зображене на рис. 3 та рис. 4.

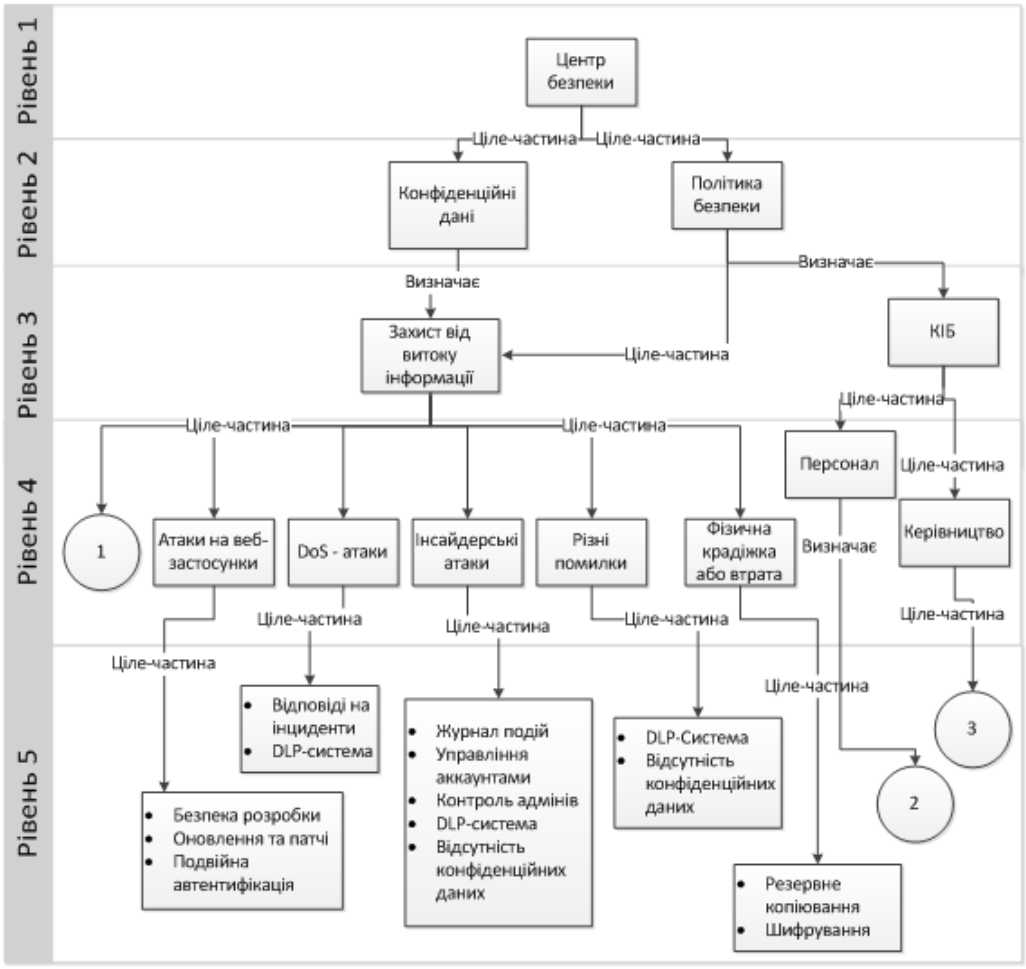

Рис. 2. Онтограф. Частина 1

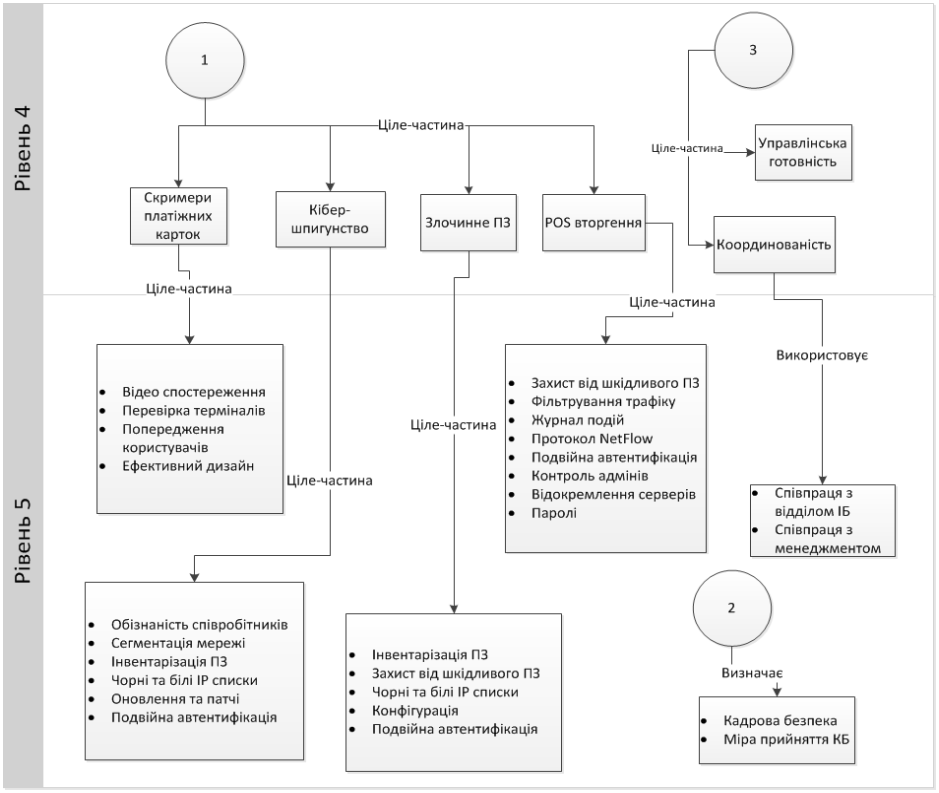

Рис. 3. Онтограф. Частина 2

Висновки. В статті проаналізовано основні загрози безпеці інформації в організації: сценарії ураження інформації та інциденти, обумовлені недостатнім рівнем культури інформаційної безпеки, що мають відношення до загроз, пов'язаних з людськими чинниками. В результаті проведеного аналізу визначено множини типових подій та відношень між ними, необхідні для побудови онтографу - логіко-семантичної схеми, що візуалізує взаємозв'язки та черговість робіт із створення КСЗІ. Отримана онтологічна структура дозволяє, враховуючи можливі сценарії реалізації загроз інформації, визначені дослідженням відомостей щодо інцидентів в області інформаційної безпеки із врахуванням стану культури інформаційної безпеки організації, підібрати та взаємоузгодити комплекс засобів і заходів захисту. Побудований онтограф може використовуватися як базова модель для аналізу ефективності КСЗІ організації, для визначення її узагальненої формальної оцінки захищеності у інформаційній сфері, автоматизації процесу визначення цієї оцінки.

ЛІТЕРАТУРА

[1]. T. Gruber, "A translation approach to portable ontologies", *Knowledge Acquisition*, №5(2), С. 199-220, 1993.

[2]. А. Никоненко, "Обзор баз знаний онтологического типа", *Штучний інтелект*, № 4, С. 208-219, 2009.

[3]. А. Палагин, Н. Петренко, К. Малахов, "Методика проектирования онтологии предметной области", *УСиМ*, с. 14, 2009.

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

[5]. 2016 Data Breach Investigation Report, Verizon Enterprise Solutions, [Електронний ресурс]. Режим доступу: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf [Дата доступу: травень 2017].

[6]. 2015 Data Breach Investigation Report, Verizon Enterprise Solutions, [Електронний ресурс]. Режим доступу: https://iapp.org/media/pdf/resource_center/Verizon_data-breach-investigation-report-2015.pdf [Дата доступу: травень 2017].

[7]. 2013 Data Breach Investigation Report, Verizon Enterprise Solutions, [Електронний ресурс]. Режим доступу: http://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_en_xg.pdf [Дата доступу: травень 2017].

[8]. А. Потий, Д. Пилипенко, И. Ребрий, "Предпосылки к формированию культуры информационной безопасности и метод комплексного оценивания ее уровня", *Радіоелектронні і комп'ютерні системи*, №5(57), С. 72-77, 2012.

[9]. Д. Майерс, *Социальная психология.* СПб.: Питер, 2002.

[10]. J. VanNiekerk, "Fostering Information Security Culture through Integrating Theoryand Technology", PhD thesis, Nelson Mandela Metropolitan University, 2010.

REFERENCES

[1]. T. Gruber, "A translation approach to portable ontologies", *Knowledge Acquisition*, vol. 5, no. 2, pp. 199-220, 1993.

[2]. A. Nikonenko, "The Ontological Knowledge Bases Review", *Artificial Intelligence*, no. 4, pp. 208-219, 2009.

[3]. A. Palagin, N. Petrenko, K. Malakhov, "Technique for designing a domain ontology", *Control systems and machines*, p. 14, 2009.

[4]. O. Arkhypov, "As for methods of identification and evaluation of assets information technology systems", *Information Security*, no. 1(50), pp. 42–47, 2011.

[5]. 2016 DataBreach Investigation Report, Verizon Enterprise Solutions, [Online]. Available: http://www.verizonenterprise.com/resources/reports/ rp_DBIR_2016_Report_en_xg.pdf [Дата доступу: травень 2017].

[6]. 2015 DataBreach Investigation Report, Verizon Enterprise Solutions, [Online]. Available: https://iapp.org/media/pdf/resource_center/Verizon_data-breach-investigation-report-2015.pdf [Дата доступу: травень 2017].

[7]. 2013 Data Breach Investigation Report, Verizon Enterprise Solutions, [Online]. Available: http://www.verizonenterprise.com/resources/ reports/rp_Verizon-DBIR-2014_en_xg.pdf [Accessed: May-2017].

[8]. A. Potiy, D. Pilipenko, I. Rebriy, "The prerequisites of information security culture development and an approach to complex evaluation of its level", *Radioelectronic and computer systems*, no. 5(57), p. 72 – 77, 2012.

[9]. D. Myers, *Social psychology*. NewYork: McGraw-Hill, 1983.

[10]. J. VanNiekerk, "Fostering Information Security Culture through Integrating Theoryand Technology", PhD thesis, Nelson Mandela Metropolitan University, 2010.

ПРИМЕНЕНИЕ ИНФОРМАЦИОННОЙ ОНТОЛОГИИ ДЛЯ ПРОЕКТИРОВАНИЯ И АНАЛИЗА КСЗИ

В статье предлагается вариант онтологической структуры как специфической формально-логической схемы, позволяющей накапливать и упорядочить сведения о типичных угрозах информации, методах и средствах их нейтрализации, анализировать эффективность возможных вариантов построения системы защиты информации. Формирование онтологии выполняется с ориентацией на наиболее распространенные варианты сценариев реализации угроз информации и типичные уязвимости организации, обусловленные характерным для нее состоянием и уровнем культуры информационной безопасности. Данная онтологическая структура может быть использована для вычисления значений информационных рисков для типовых сценариев реализации угроз информации, формирование базовой системы защиты информации и определения обобщенной оценки защищенности организации в информационной сфере.

Ключевые слова: онтологическая структура, оценка риска, сценарии утечки информации, культура информационной безопасности, онтограф, угрозы информации, уровень информационной культуры.

ONTOLOGICAL STRUCTURE APPLICATION FOR ANALYSIS AND DEVELOPMENT OF CISS

The article proposes ontological structure variant for analysis of CISS, which focuses on the most common information security leaks scenarios and information security culture. The analysis of CISS is based on many factors (attack scenarios on the system, etc.), many of which also depend not only on hardware elements. Common errors and misunderstanding of the security incidents definition and how to react also play an important role. So, for basic security system assessment evaluation, structure, that has determined factors and scenarios of CISS analysis for further use will greatly simplify understanding and automating processes of these evaluations. Proposed ontological structure can be used to determine average risk of information leakage scenarios and to determine information security culture level to specify overall formal security assessment of organization and, as such, to automate the process of determining this assessment.

Keywords: ontological structure, risk assessment, information leakage scenarios, information security culture, ontograph, information threat, information security culture level.

Архипов Олександр Євгенійович, доктор технічних наук, професор кафедри інформаційної безпеки НТУУ «КПІ імені Ігоря Сікорського».
E-mail: sonet0515@gmail.com

Архипов Александр Евгеньевич, доктор технических наук, профессор кафедры информационной безопасности НТУУ «КПИ имени Игоря Сикорского».

Arkhypov Oleksandr, Professor, Doctor of Sciences in Eng., professor of the Department of Information Defense of National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

Козленко Олег Віталійович, аспірант кафедри інформаційної безпеки ФТІ, НТУУ «КПІ імені Ігоря Сікорського».
E-mail: education.kozlenko@gmail.com

Козленко Олег Віталійович, аспирант кафедры защиты информации ФТИ, НТУУ «КПИ имени Игоря Сикорского».

Kozlenko Oleh, PhD student of the Department of Information Defense, IPT, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".