

ПРИКЛАД ПОБУДОВИ ОНТОЛОГІЧНОЇ СТРУКТУРИ СТАНДАРТІВ У ОБЛАСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ПОДАЛЬШОГО ОЦІНЮВАННЯ ВАРТОСТІ ВТРАТ

О. В. Козленко¹, О. Є. Архипов¹

¹Національний технічний університет України «Київський політехнічний інститут»

Анотація

У статті викладається метод поетапного аналізу та оцінки втрат та реалізація онтології стандартів по оцінюванню ризиків для подальшого визначення вартості втрат за допомогою онтологічного методу визначення

Ключові слова: онтологія, оцінювання ризику, оцінювання вартості втрат

Вступ

В роботі досліджуються теоретичні засади оцінювання вартості втрат, які зумовлені реалізацією інформаційних загроз, та структуроване представлення взаємодії стандартів оцінювання ризиків для конкретного підприємства. В результаті дослідження виявилось, що проблема структурованого представлення взаємодії стандартів оцінювання ризиків є актуальною. Тому метою роботи є розробка та впровадження цієї структури. Наукова новизна роботи полягає в пропозиції структурованого підходу та побудови онтологічної структури взаємозв'язку стандартів з оцінювання ризиків та менеджменту системи захисту інформації завдяки цим стандартам.

1. Теоритичні основи побудови онтології

Згідно з [1, 2, 3] комп'ютерна онтологія – це формальне вираження концептуальних знань про предметну область і за своєю значимістю порівняна з базою знань інтелектуальної інформаційної системи, а її побудова є специфічною формою людського мислення. У простому випадку методика проектування онтології Пдо включає три етапи проектування:

- Попередній аналіз заданої Пдо
- Побудова вручну онтографу Пдо
- Графічне (візуальне) проектування онтографу Пдо і складання формалізованого опису онтології Пдо

$$O = \langle X, R, F \rangle,$$

де $X = \{x_1, x_2, \dots, x_i, \dots, x_n\}$, $i = \overrightarrow{1n}$,

$n = \text{Card}X$ – кінцева множина концептів(понять) заданої Пдо;

$R = \{r_1, r_2, \dots, r_k, \dots, r_m\}$, $R = x_1 * x_2 * \dots * x_n$,

$k = \overrightarrow{1m}$, $n = \text{Card}R$ – кінцева множина семантично значущих відносин між концептами Пдо.

Вони визначають тип взаємодії між поняттями. У загальному випадку, відносини ділять на загальнозначущі (з яких виділяють, як правило, відносини часткового порядку) і конкретні відносини заданої

Пдо. $F = X * R$ – кінцева множина функцій інтерпретації, заданих на концептах або відносинах. Окремим випадком завдання множини функцій інтерпретації F є глосарій, складений для множини понять X . Під онтографом розуміється двочастковий граф, вершинами якого є поняття Пдо, а дугами – зв'язки між ними. Метою побудови є загальноприйнята і загальнодоступна концептуалізація певної області знань (світу, середовища), яка містить базис для моделювання цієї області знань і визначає протоколи для взаємодії між агентами.

2. Опис виробництва

Як відомо, виробництво – це сукупність взаємопов'язаних процесів: основних, допоміжних і обслуговуючих. Основними є технологічні процеси (ТП) виробництва, завдяки ним і утворюється матеріальний продукт – основний результат виробництва.

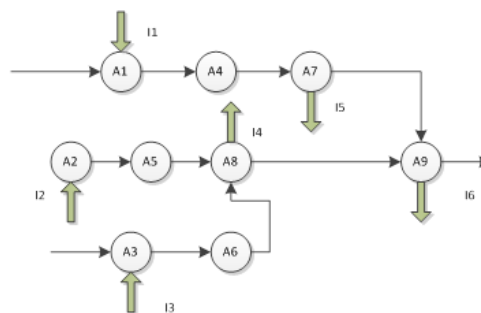


Рис. 1. Схема ТП

В зв'язку з цим формування онтологічної інформаційної ієрархії треба починати з аналізу найнижчих етапів виробництва, тобто з визначення інформації, задіяної у основних виробничих процесах. Зокрема, якщо мова йде про певне матеріальне виробництво, починати треба з аналізу його основних ТП.

Для прикладу надано підприємство (рис. 1) [3, 4] яке апаратно підсумовує інформацію, яку надає клієнт, інформацію про зовнішні та внутрішні фактори

Табл. 1. Етапи визначення втрат

Етапи	Опис
1	Виконується інвентаризація активів організації, підсумок якої – список активів, визначає повну множину активів організації: $AS = \{as_i\}$, $i = \overline{1n_A}$. Потім встановлюється перелік можливих загроз інформації: $T = \{t_k\}$, $k = \overline{1n_t}$. Формується підмножина $AS_{inf1} \subset (AS_{inf})$
2	Виконується аналіз всіх можливих пар виду $\langle as_i^{inf1}, as_i \rangle$, за результатами якого визначаються групи активів, асоційованих з кожним елементом as_i^{inf1} інформаційних ресурсів, щодо якої може бути реалізована загроза
3	виявляються втрати для активів as_i , організації у разі реалізації загрози t_k щодо інформаційного ресурсу as_i^{inf1} , і за сукупним значенням всіх цих втрат, обчисленим по всій множині активів AS , визначають часткову цінність відповідного інформаційного ресурсу

та за допомогою алгоритмів робить висновок, де І1 – інформація клієнта, І5 – результат обробки інформації клієнта, І2 – інформація про зовнішні фактори, І3 – інформація про внутрішні фактори, І4 – систематизований висновок про внутрішню та зовнішню інформацію, І6 – результат обробки. А1 – обробник інформації клієнта, А4 – алгоритм для інформації клієнта, А7 – база даних з інформацією клієнта, А2 – обробник інформації зовнішніх факторів, А5 – алгоритм для зовнішньої інформації, А8 – база даних з сукупної інформацією про фактори, А3 – обробник внутрішньої інформації, А6 – алгоритм для внутрішньої інформації, А9 – алгоритму для висновку на основі клієнтської інформації та систематизованої інформації. Формально з урахуванням зазначених вище аспектів схему оцінювання збитку можна представити у вигляді триетапної процедури (Табл. 1). Згідно з [4] при її побудові будемо виходити з того факту, що в організації об'єктами введення загроз інформації є елементи інформаційної інфраструктури (обладнання, програмне забезпечення, персонал), які через присутність в них вразливостей створюють можливості для реалізації тих чи інших атак, щодо інформаційних ресурсів. Для отримання працездатної процедури оцінки активів необхідно ввести механізми скорочення кількості варіантів пар <актив–загроза> до розумно прийнятного кількості. Одним з таких механізмів є метод сценарного аналізу втрат, обумовлених реалізацією загроз щодо певного інформаційного ресурсу. Згідно з [4] у цьому методі експерт для кожного ймовірного випадку реалізації загрози визначає кінцеву множину можливих сценаріїв розвитку подій-наслідків (3 – 5 варіантів). Розгортання кожного з сценаріїв асоціюється з деяким конкретною множиною активів, яка за своїм обсягом менша ніж гіпотетична повна група активів. Тому експерт здатний досить об'єктивно оцінити наслідки розвитку кожного сценарію, які фактично складуть приватні інтегровані оцінки збитку(втрат), обумовленого реалізацією вихідної загрози.

3. Характеристика стандартів та побудова онтологічної структури

Використання сценарного підходу спирається на генерацію сценаріїв, які породжуються загрозами.

Загрози виявляються через аналіз порушень політики безпеки і технічних специфікацій. Для знаходження порушень політики безпеки проводять аудит по ISO 17799 (зараз – 27001, а їх адаптація до сфери аудиту – 17021, 19001 (після адаптації 19001 в сферу інформаційної безпеки він перетворився на 27007)). Для виконання аналізу фахівцем складається онтологія, елементами якої будуть як стандарти, так і їх розділи або пункти. Для побудови онтології ми визначимо необхідні для нас стандарти оцінювання ризиків та визначимо взаємозв'язок між ними (Табл. 2).

Стандарт управління визначає, як запустити систему, а в разі ISO 27001[6], він визначає систему управління інформаційною безпекою (СУІБ). Тому, якщо дивитися на деталі цього стандарту, він вимагає, що інформаційна безпека повинна бути реалізація, моніторинг, відгуки, а також поліпшення. Він також встановлює чіткі обов'язки, де мають бути встановлені цілі, елементи управління, внутрішні аудити, які документи знаходяться під контролем, які записи перебувають під контролем і так далі. В ISO 27002[7] наведено список елементів управління. Тобто встановленні конкретні дії для забезпечення вимог з ISO 27001. Також слід відзначити, що ISO 27002 не визначає, які елементи управління застосовні до якої організації. ISO 27001 відзначає, що управління інформаційної безпеки в ISO 27001 суміщене з ISO 31000[8]. Тому ISO 27001 не говорить, що потрібно реалізувати обстеження і лікування небезпеки відповідно до ISO 31000, тільки говорить, що всі вимоги від ISO 27001 вже є в ISO 31000. Таким чином, можливо реалізувати управління ризиками в будь-якому випадку, поки він відповідає ISO 27001. Також різниця між ISO 27001 та ISO 31000 полягає в специфіці. В ISO 27001 можливо визначити і виміряти, наскільки конкретний елемент управління працює на відміну від ряду інших спільних стандартів. У рамках аналізу потрібно буде виконати оцінку ризику, в якій слід чітко визначити стан активу та його контрольне середовище. Для знаходження порушень технічних специфікацій проводять аудит по ISO 15408. Для сценарного розрахунку ризиків визначають стратегію аналізу ризиків (13335 –3), потім методики розрахунку – 31000, 31100, 31010 (їх адаптація в ІБ – 27005, 27004), деталізацією є NIST.

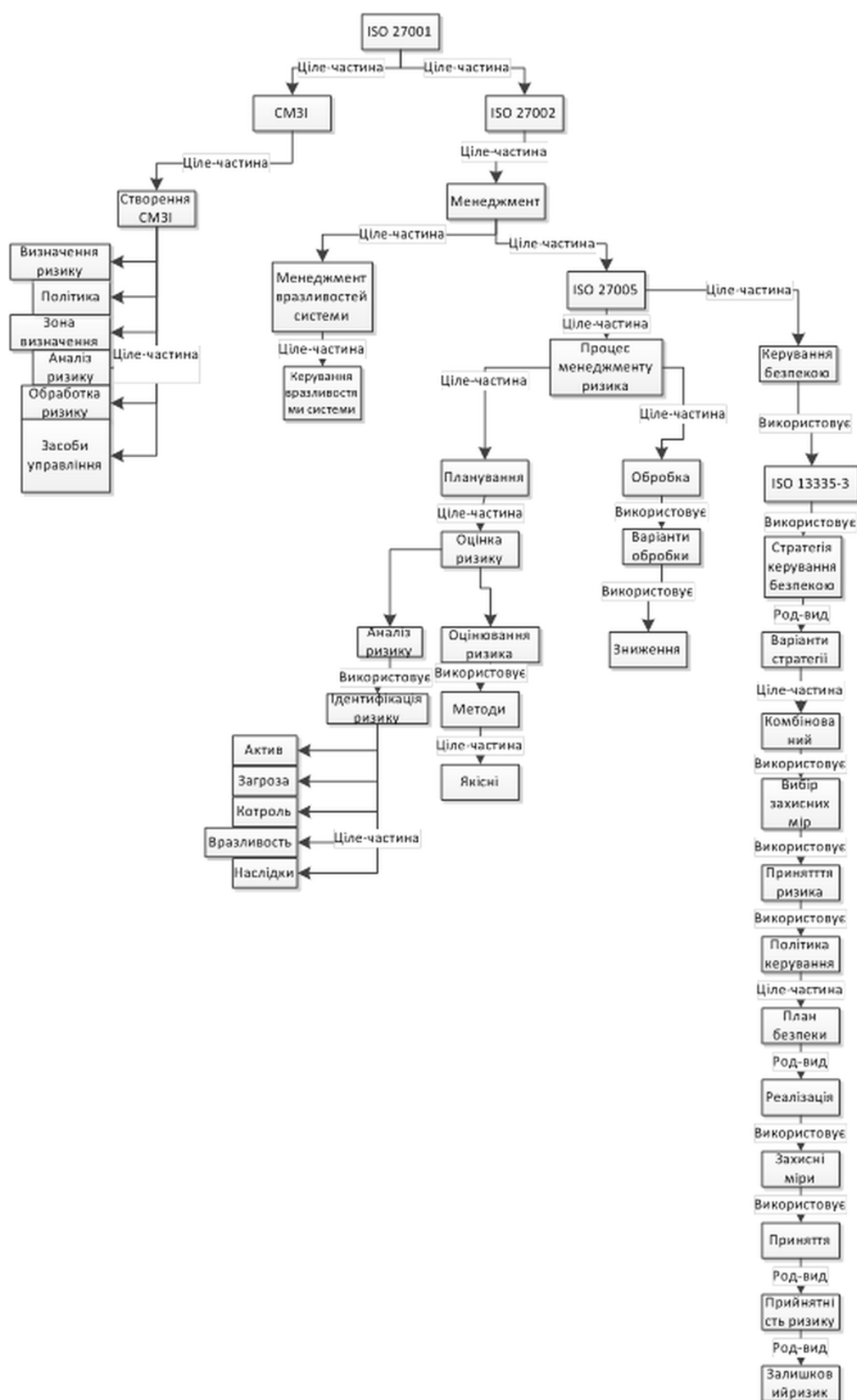


Рис. 2. Онтологія стандартів оцінювання ризиків для підприємства

Табл. 2. Характеристика стандартів

ISO	Мета	Зв'язок
27001	Визначає систему управління інформаційною безпекою (СУІБ)	Базовий
27002	Список елементів управління	ISO 27001
27005	Кращі практики управління ризиками	ISO 27001, ISO 27002
31000	Керівні принципи в області управління ризиками	Еквівалент ISO 27005
13335–3[5]	Описи і рекомендації ефективного управління безпекою	Частина ISO 27005

Різниця між ISO 27005[9] та ISO 31010 полягає у тому, що 27005 стандарт забезпечує рекомендації для менеджменту ризиків інформаційної безпеки, які включають інформацію та менеджмент ризиків безпеки технологій телекомунікації, а ISO 31010 містить рекомендації щодо вибору і застосування методів оцінки ризику, не призначений для цілей оцінки відповідності та використання в якості обов'язкових або договірних вимог, не містить конкретних критеріїв для прийняття рішення з аналізу ризику та вказівок щодо застосування методів аналізу ризику в конкретній ситуації, не пов'язаний з аспектами безпеки.

Отже, визначивши усі необхідні нами елементи, зв'язки та інше ми будемо необхідну онтологічну структуру, яка повністю описує наше підприємство і може використовуватися у подальшому оцінюванню вартості втрат (рис. 2).

Висновки

Стратегічним елементом управління інформаційною безпекою організації є правильний вибір прийнятного рівня ризику. Цей вибір безпосередньо залежить від цілей, які ставить перед собою організація при створенні системи захисту інформації та необхідність вивчити активи організації і визначити їх цінність для неї. Це потрібно не тільки для формулювання та оцінки цілей організації а також і для визначення вартості втрат, які будуть зумовлені реалізацією загроз на ці активи. Стандарти оцінювання інформаційних ризиків дають різну інформацію щодо побудов систем захисту інформації та визначення методів оцінювання та менеджменту ризиків але чіткої узагальненої структури представлення цих стандартів на сьогоднішній час на жаль немає для подальшого використання у оцінці вартості втрат. Для вирішення цієї проблеми була зроблена онтоло-

гічна структура зв'язку, складу та взаємодії стандартів ISO 27001, ISO 27002, ISO 27005, ISO 31000, ISO 31010, ISO 13335–3 для структурованого представлення використання стандартів для конкретної організації для подальшого використання у оцінці втрат підприємства, зумовлених реалізацією інформаційних загроз.

Перелік використаних джерел

1. Палагин А.В., Петренко Н.Г. Методика проектирования онтологии предметной области // УСиМ. — 2009. — 14 с.
2. Палагин А.В., Яковлев Ю.С. Системная интеграция средств компьютерной техники. — Вінниця: Універсум, 2005. — 680 с.
3. Корченко А.Г., Архипов А.Е., Казмирчук С.В. Анализ и оценивание рисков. информационной безопасности — Вінниця: Універсум, 2005. — 680 с.
4. Архипов О.Є. Щодо методики ідентифікації та оцінювання активів системи інформаційних технологій — Захист інформації. — 2011. — №1 (50). — 47 с.
5. ГОСТ Р ИСО/МЭК ТО 13335 – 3 – 2007 «Методы и засоби забезпечення безпеки. Частина 3: методи менеджменту безпеки інформаційних технологій»
6. ISO/IEC 27001 – 2008 «Інформаційні технології. Методи захисту. Системи менеджменту захисту інформації. Вимоги»
7. ISO/IEC 27002– 2005 «Інформаційні технології. Звід правил з управління захистом інформації»
8. СТБ ISO 31000 «Менеджмент ризику. Принципи та керівні вказівки»
9. ISO/IEC 27005 – 2005 «Інформаційна технологія – Методи захисту – Менеджмент ризиків інформаційної безпеки»