відповіду фахову підготовку та досвід роботи, при відповідному технічному оснащенні.

З урахуванням зазначеного всі суб'єкти системи ТЗІ, які проваджують свою діяльність у сфері ТЗІ, мають пройти відповідну атестацію: суб'єкти господарської діяльності отримують ліцензію відповідно до Закону України "Про ліцензування певних видів господарської діяльності" (на сьогодні ліцензії на право провадження господарської діяльності у сфері ТЗІ мають більше 200 суб'єктів господарювання), а державні орагни – дозволи на право преведення робіт з ТЗІ для власних потреб.

Крім цього, в державі створено систему підготовки, перепідготовки та підвищення кваліфікації фахівців з питань захисту інформації (на сьогодні 20 вищих навчальних закладів здійснюють підготовку спеціалістів в сфері забезпечення захисту інформації).

Обов'язковою умовою забезпечення захисту інформації, яка циркулює в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності, є одержання об'єктивної оцінки рівня захищеності інформаційної, що здійснюється через систему деражвної експертизи та атестації.

Ефективність робіт з технічного захисту інформації може бути досягнута при умові застосування захищених засобів обробки інформації та засобів її захисту, які мають відповідні серитфікати та експертні висновки. Для цього зазначені засоби, які надходять на український ринок і споживачі яких належать до державної сфери, проходять атестацію на відповідність вимогам ТЗІ в Українській державній системі сертифікації продукції УкрСЕПРО, для чого створені та акредитовані в цій системі огран з сертифікації та випробувальні лабораторії, а також через систему державної експеертизи (на сьогодні до переліку засобів загального призначення, які дозволені для забезпечення ТЗІ, включено 257 засобів, з них – 144 за принципом дії не створюють канали витоку оброблюваної інформації).

Також важливе місце в системі ТЗІ відіграє державний контроль за її функціонуванням, який здійснюється шляхом проведення перевірок виконання вимог нормативно-правових актів у сфері ТЗІ в органаз деражвної влади, органаз місцевого самоврядування, відповідних підприємствах, установах та організаціях.

Таким чином, існуюча на сьогодні в Україні система ТЗІ дозволяє вирішувати практично весь комплекс завдань з ТЗІ з обмеженим доступом на об'єктах інформаційної діяльності та в інформаціно-телекомунікаційних системах державних органів, підприємтв, установ та організацій, дозволяє забезпечити розвиток матеріально-технічної бази ссистеми технічного захисту інформації.

Разом з тим, якісні зміни, що відбуваються в сферах життєдіяльності особи, суспільства, держави та супроводжуються постійним зростанням ролі інформаційних технологій, потребують своєчасної розробки і реалізації заходів щодо розвитку системи ТЗІ.

Сьогодні серед основних напрямків розвитку системи ТЗІ в Україні найбільш пріоритетними можна відмінити наступні:

- визначення шляхів упорядкування та оптимізації заходів щодо створення, експертизи та впровадження в експлуатацію автоматизованих систем державних установ, призначених для обробки інформації, що становлять державну таємницю;
- підвищення безпеки вітчизняних інформаційних ресурсів шляхом розроблення та впровадження в автоматизованих системах державних органів та уствно вітчизняної захищеної операційної системи;
- створення сучаних нормативних документів з питань захисту інформації від витоку технічними каналами, визначення підходів щодо створення та впровадження комплексів ТЗІ на об'єктах інформаційної діяльності;
- удосконалення організаційної структури захисту інформації в державних органах та установах;
- активаці інформаційно-аналітичної роботи в інтересах ефективного вирішення актуальних проблем у сфері ТЗІ;
- розширення номенклатури вітчизняних засоібв забезпечення ТЗІ.

УДК 681.3.06

МЕТОДИКА ФОРМУВАННЯ ВЕРБАЛЬНИХ ОЦІНОК ЩОДО ЗАХИЩЕНОСТІ ІТС НА ОСНОВІ ВИМОГ НОРМАТИВНИХ ДОКУМЕНТІВ

Олександр Потій, Анатолій Лєншин

ЗАТ „Інститут інформаційних технологій"

Анотація: **Пропонується методика формування вербальних оцінок зрілості процесів з забезпечення**

безпеки інформації. Використовується математичний апарат суб'єктивної логіки та зони базових думок.
Summary: **The verbal estimates forming method of information security process maturity are proposed. The mathematical tool of subjective logic and base regions are used.**
Ключові слова: **Безпека інформації, суб'єктивна логіка, вербальні оцінки, функції належності, збір знань, математичний апарат, зона базових думок.**

Вступ

Оцінка зрілості процесів з забезпечення безпеки інформації є одним із підходів проведення аудиту безпеки. Типовим вирішенням проблеми формування переліку процесів та вимог до них є застосування національних та міжнародних стандартів у галузі захисту інформації. Підвищення якості та швидкості проведення оцінки, а також спрощення роботи аудитора може бути досягнуто шляхом її автоматизації. Автоматизована система має задовольняти певному переліку вимог, що висуваються до таких систем, це коректність обробки результатів, зручність збору вихідних даних та наочність представлення результатів тощо. Остання властивість досягається як графічним інтерфейсом так і можливістю видачі результатів природною мовою аудитора чи замовника оцінки.

I Аудит безпеки інформації. Формалізація процесу оцінки,
вибір математичного апарату

Невід'ємною складовою життєвого циклу захищених ІТС є проведення аудиту безпеки інформації. Відповідальному за проведення аудиту безпеки інформації необхідно вирішити такі питання: визначення моделі порушників, формування переліку загроз, складання чи використання існуючої методики збору інформації щодо захищеності ІТС, обробка отриманої інформації та звітування з результатів аудиту. З метою полегшення цієї діяльності багатьма дослідницькими інститутами розроблюються інструкції та методики, що містять практичні поради щодо реалізації того чи іншого кроку. Стандарт звичайно містить методику проведення оцінки безпеки та додатки, в яких наведено переліки загроз, вимог безпеки тощо. Вимоги безпеки структуруються у вигляді ієрархічного дерева в корені якого знаходиться задача захисту в цілому, а листи являють собою так звані кращі практики. В загальному випадку дерево може містити довільну кількість рівнів, але на практиці найчастіше застосовують 4 - 5 рівневі дерева. На сучасному етапі, організації, що займаються розробкою подібних документів, не дійшли до згоди щодо однозначного найменування цих рівнів, але змістовне навантаження у різних стандартах однакове.

Національний інститут стандартизації та технологій [1] пропонує систематизувати вимоги безпеки наступним чином (рис. 1). Як видно з рисунка для задачі (цілі) першого рівня проводиться декомпозиція на три підцілі з урахуванням основних областей (сфер), в яких здійснюється захист інформації. Підцілі отримують назви, що відповідають назвам цих областей. Усі практичні роботи з забезпечення безпеки інформації, що здійснюються в області, можна класифікувати за напрямками (напрямок управління ризиками, напрямок захисту персоналу, напрямок з забезпечення цілісності даних тощо). Отже цілями третього рівня є напрямки практичної діяльності з забезпечення безпеки інформації. Ефективне виконання задач, покладених на службу захисту інформації держави та окремих установ, не може здійснюватися лише власними цілями, необхідним є застосування досвіду провідних компаній світу. Такий досвід представляється в стандартах у вигляді кращих практик. Зважаючи на стрімкий розвиток інформаційних технологій вирішення задачі забезпечення безпеки інформації носить все більш комплексний характер, отже виконання окремих робіт, навіть кращих, не може забезпечити задовільний результат. Для рішення задач захисту з кращих практик формуються комплекси практичних робіт, що складаються із набору кращих практик, виконання яких забезпечує базовий рівень захищеності.

При адаптації до потреб конкретної установи комплекси робіт можуть бути розширені специфічними вимогами. Такі комплекси з забезпечення безпеки інформації є цілями четвертого рівня. Кінцевими листовими цілями – є кращі практики. Робота аудитора безпеки зводиться до перевірки якості виконання робіт у комплексах і накопичення матеріалу, який буде застосовуватися при оцінці ступеню виконання задачі безпеки як в цілому, так і за окремими напрямками. В загальному вигляді процес оцінки представлено на рис. 2 у вигляді схеми SADT (технології системно-структурного аналізу) [2].

Згідно з вимогами SADT – назва процесу, що модулюється, пишеться у прямокутнику, а над стрілками пишуться дані, що використовуються або виникають у ході даного процесу. Зліва від прямокутника пишуться вхідні дані, зверху –дані з керування (ті, що впливають на хід протікання процесу), зправа – дані, отримані в ході процесу, знизу – допоміжні засоби або умови, необхідні для здійснення процесу.

Великий обсяг інформації, який необхідно обробляти при проведені аудиту (під обробкою розуміється збір, розрахунок узагальнених оцінок та значень кількісних показників, зберігання і накопичування

інформації тощо), та значна кількість рутинної роботи зумовлює необхідність автоматизації процесу проведення аудиту. Швидкоплинність процесів із забезпечення захисту інформації, а також апріорна неможливість охоплення усіх деталей реалізації викликає певну ступінь невизначеності або невпевненості у оцінках аудитора безпеки (далі експерта). Отже математичний апарат, що буде використовуватися як основа в автоматизованій системі повинен забезпечувати можливість надання оцінок, що враховують цю невизначеність, та їх коректної обробки. На роль такого математичного апарату можуть претендувати методи нечітких множин, апарат суб'єктивної логіки, логіко-імовірнісний підхід тощо.

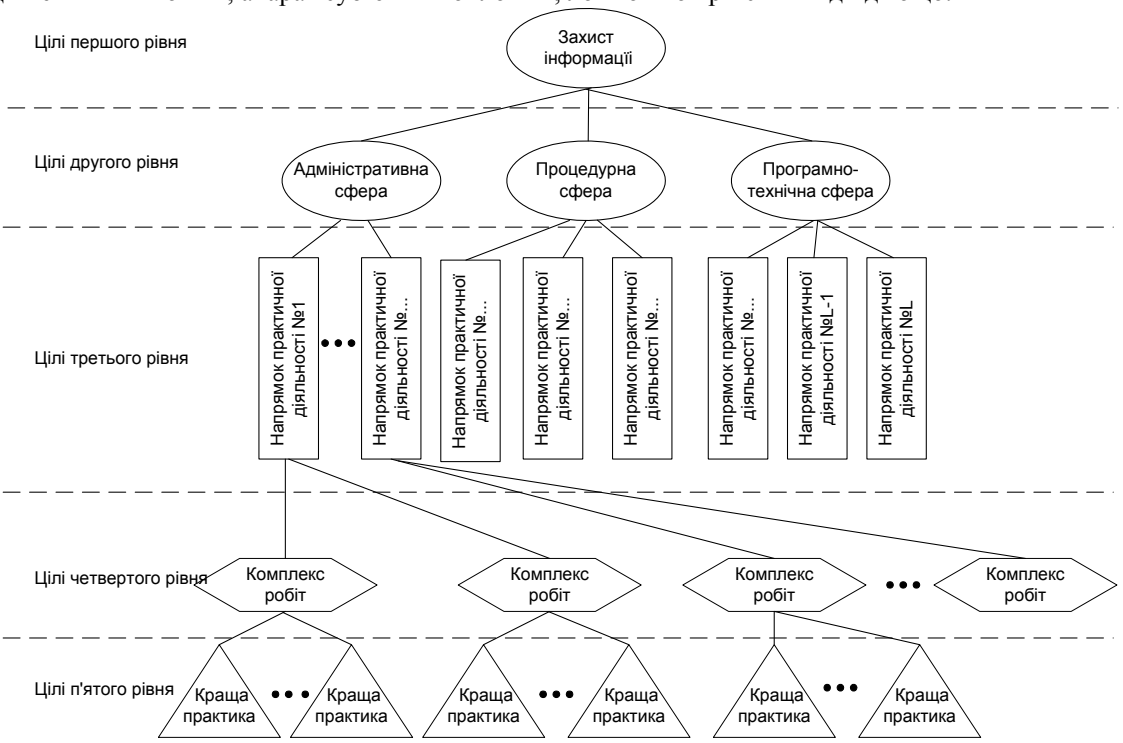


Рисунок 1 – Систематизації вимог безпеки NIST

У ідеальному випадку при наданні оцінок експертом можуть виникнути три граничні ситуації:

- процес здійснюється відповідно до вимог, що висуваються до нього;
- процес здійснюється без урахування жодної вимоги, або не здійснюється зовсім;
- у оцінювача немає ніякої інформації відносно протікання процесу, або вимог, що висуваються до нього.

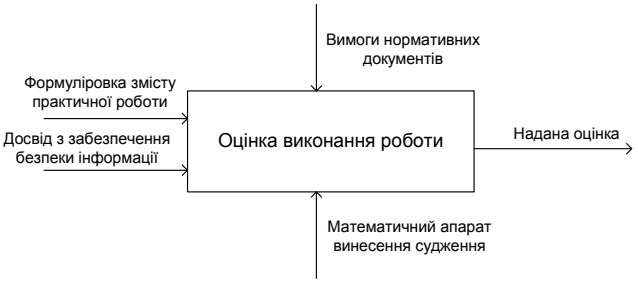


Рисунок 2 – SADT схема процесу оцінки

Для кожної з цих ситуацій експерт може надати граничну оцінку із сто відсотковою впевненістю „процес виконується", „процес не виконується", „не знаю, чи виконується процес" відповідно. На практиці усі оцінки експерта будуть лежати десь між цими граничним оцінками. Виходячи з цього як математичний апарат пропонується використовувати суб'єктивну логіку [3 - 9]. Центральним положенням суб'єктивної логіки є оперування трьома параметрами. Параметри ці позначають ступінь довіри (b), недовіри (d) та невизначеності (u) у думці, що висловлюється стосовно вірності будь-якого довільного твердження. Отже, якщо висловити твердження, що на об'єкті оцінки виконується певна функція безпеки (процес

здійснюється відповідно до висунутих вимог), то параметри думки у просторі суб'єктивної логіки наберуть такі значення. Довіра, яку експерт призначає твердженню про коректність реалізації та протікання процесу, позначає ступінь з якою експерт вважає, що процес виконується. Природа недовіри навпаки виходить з того, що експерт знає чи підозрює, що виконання вимоги безпеки не здійснюється на належному рівні, отже значення недовіри - це ступінь, з якою експерт вважає, що вимога не виконується. Параметр невизначеності вказує на неповноту знань експерта, яка може бути зумовлена як недостатньою кваліфікацією експерта для проведення оцінки подібного роду так і неможливістю врахування на даному етапі всіх аспектів проблеми з об'єктивних причин (відсутністю відповідальних за цей аспект осіб, недоступність для вивчення усього обсягу інформації або нехватка часу для такого вивчення тощо). Пропозиції, щодо можливості застосування суб'єктивної логіки при проведенні аудиту безпеки інформації наведено у табл. 1.

Таблиця 1 – Порівняння змістовного значення параметрів суб'єктивної логіки

	Що позначає	
	у стандартному застосуванні	в галузі захисту інформації при оцінці захищеності
Об'єкт оцінки	довільне твердження	твердження про коректність процесу захисту інформації, що оцінюється
Довіра	ступінь, з якою оцінювач погоджується з ним, тобто довіряє його істинності	ступінь, з якою на думку експерта виконується даний процес
Недовіра	ступінь з якою оцінювач не згоден з твердженням, тобто недовіряє його змісту	ступінь, з якою на думку експерта даний процес не виконується
Невизначеність	невизначеність експерта щодо істинності твердження	невизначеність експерта щодо коректності процесу
Що перевіряється	Істинність твердження	ступінь виконання, невиконання процесів та невизначеність при наданні оцінок

Сформуємо загальну постановку задачі, яку має вирішувати обраний математичний апарат при проведені аудиту безпеки інформації.

Нехай $O = \{O_1, O_2, O_3, .., O_m\}$ – множина вербальних відповідей, які може надавати експерт, де m – мінімальна кількість відповідей, якої достатньо для оцінки будь-якого стану об'єкту оцінки. $W = \{\omega_1, \omega_2, \omega_3, ..\omega_m\}$ – це відображення цих оцінок у просторі суб'єктивної логіки у вигляді суб'єктивних думок. Необхідно сформувати таку функцію G, що забезпечить однозначне перетворення $G(O_i) = \omega_i$ де $O_i \in O; \omega_i \in W; i = \overline{1..m}$ та зворотну функцію G^{-1}, за допомогою якою можна буде провести однозначне зворотне перетворення $G^{-1}(\omega_i) = O_i$ де $O_i \in O; \omega_i \in W; i = \overline{1..m}$

Таким чином загальна постановка задачі оцінки має такий вигляд (рис. 3).

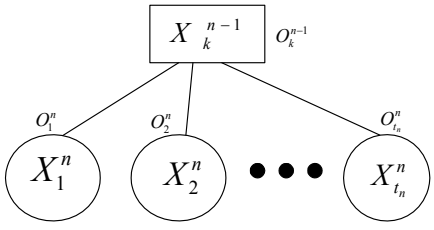


Рисунок 3 – Графічне представлення постановки задачі оцінки

Необхідно отримати експертні оцінки ступеня виконання кожного процесу X_j^n (де n –номер рівня у дереві цілей, j –порядковий номер процесу) у просторі формалізованих вербальних оцінок $O_j^n \in O$, (де n –номер рівня у дереві цілей, j –порядковий номер процесу). На наступному кроці перевести оцінки у простір суб'єктивної логіки за допомогою функції G, та обробити за допомогою спеціальних операторів. Отриману в такий спосіб оцінку X_k^{n-1} для вищого рівня перевести в область вербальних оцінок O.

Розглянемо можливість вирішення сформульованих задач математичним апаратом суб'єктивної логіки.

Для переходу від вербальних оцінок до оцінок у вигляді параметрів суб'єктивної логіки пропонується використати базові зони думок, на які можна розбити весь трикутник думок. Тобто як функцію G використаємо функцію, яка по номеру зони базової думки буде надавати значення середньої точки цієї зони.

Розбиття трикутника думок на базові зони (рис. 4), а також можливість висловлення експертом своєї думки шляхом вибору однієї з них обгрунтована авторами у роботі [8].

Кожна із зон характеризується сталим співвідношеннями параметрів довіри, недовіри та невизначеності. Математичний опис границь зон базових думок наведено у таблиці 2.

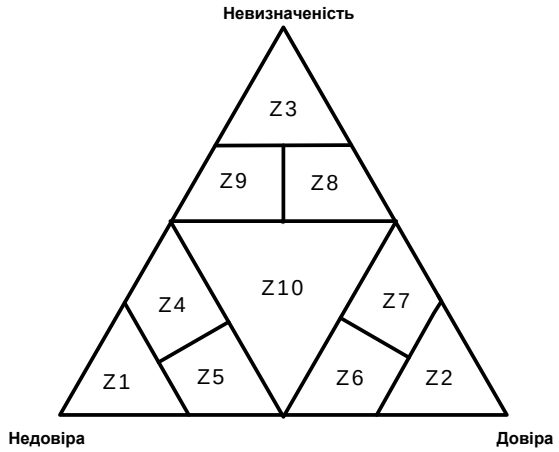


Рисунок 4 – Зони базових думок

Таблиця 2 – Математичний опис границь зон базових думок

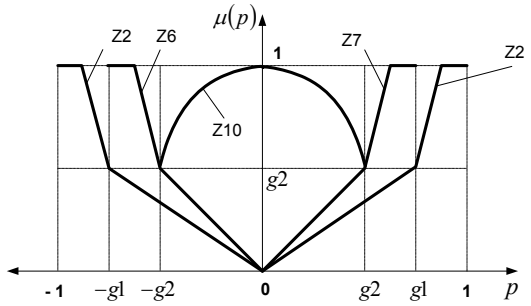
№	Математичний вираз	Типова вербальна відповідь
Z1	$d \phi\phi (b+u)$	Вважаю, що не виконується
Z2	$b \phi\phi (d+u)$	Вважаю, що виконується
Z3	$u \phi \phi (d+b)$	Інформації дуже мало (не знаю)
Z4	$d \phi (b+u),\ b \pi u$	Вважаю, що не виконується, але присутня невизначеність
Z5	$d \phi (b+u),\ b \phi u$	Вважаю, що не виконується в цілому, але дещо робиться
Z6	$b \phi (d+u),\ d \phi u$	Вважаю, що виконується, але присутні аргументи і проти
Z7	$b \phi (d+u),\ d \pi u$	Вважаю, що виконується, але присутня невизначеність
Z8	$u \phi (d+b), d \pi b$	Інформації мало, але є факти на користь того, що виконується
Z9	$u \phi (d+b), d \phi b$	Інформації мало, але є факти, які свідчать про те, що не виконується
Z10	$b \approx d \approx u$	Зона припущень

Знаки ϕ та π вказують на те, що один із операндів переважає по значущості інший чи навпаки (як операнди можуть використовуватися як один з параметрів суб'єктивної логіки так і їх комбінація). Вираз $t \phi e$ має трактуватись як "t переважає e", а не як "t більше ніж e". Це обумовлено тим, що відношення більшості є окремим випадком відношення переваги, яке визначається у кожному випадку окремо – особою, що його встановлює. Знак $\phi\phi$ позначає на значну перевагу значущості одного операнда над іншим. Результат, отриманий внаслідок використання оператора $+$, позначає не суму, а загальну значущість операндів.

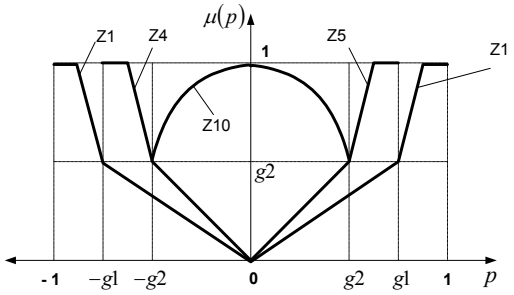
Належність думки до зони базових думок у просторі суб'єктивної логіки визначається через функцію належності (рис. 5, а-в). Для побудови функції належності думки до певної зони використовується допоміжний показник p який обчислюється за такою формулою:

$$p = \frac{t_1 - t_2}{|t_1 - t_2|} m \qquad (1)$$

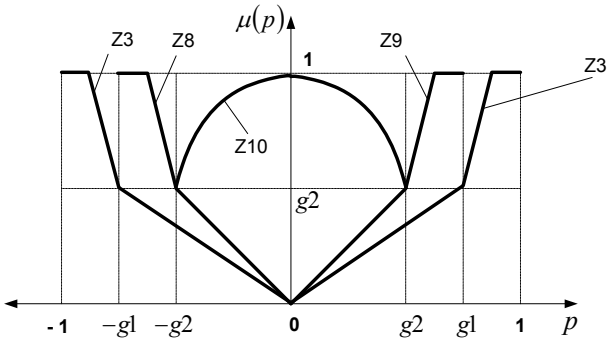
де m - головний (домінуючий) параметр, t_1 та t_2 - другорядні параметри.



а) Функції належності ($m = b \quad t_1 = d \quad t_2 = u$)



б) Функції належності для ($m = d \quad t_1 = b \quad t_2 = u$)



в) Функції належності ($m = u \quad t_1 = d \quad t_2 = b$)

Рисунок 5

Таким чином, як функція G^{-1} виступає функція належності $\mu(p)$. Тобто для перетворення значення заданого вектора думки у вербальну відповідь – оцінку, необхідно розрахувати значення допоміжного показника p, знайти номер зони, до якої належить задана думка, та сформувати вербальну відповідь-оцінку.

II Загальний підхід до формування вербальних відповідей-оцінок

Для формування вербальних відповідей-оцінок процесів, що оцінюються, пропонується поєднати зміст твердження про коректне виконання цього процесу та оцінку цього процесу у просторі суб'єктивної логіки, переведену в типову відповідь на основі зон базових думок.

Приклад:

Твердження: З метою вірного формулювання вимог безпеки проводиться первина оцінка ризиків.

Отримана оцінка: $\omega = (0.6,\ 0.3,\ 0.1)$

Розрахований номер базової зони (використовуючи функцію належності $\mu(p)$): 6.

Типова відповідь для базової зони: Вважаю, що виконується, але присутні аргументи і проти

Відповідь-оцінка: Вважаю, що в цілому з метою формулювання вимог безпеки проводиться первина оцінка ризиків, але ця оцінка не завжди є вичерпно задовільною.

На практиці при вирішенні задачі формування відповідей-оцінок для кожного із тверджень виникають труднощі, пов'язані з обробкою великого обсягу інформації. Автоматизація даної задачі може бути проведена за умови можливості представлення будь-якого вхідного твердження у формалізованому вигляді та наявності процедури (правил) формування типових відповідей на основі обробки вхідних даних. Пропонується вхідні твердження та відповіді представити у вигляді лінгвістичних змінних, що мають визначену структуру.

Дослідження принципів побудови тверджень дозволило виділити такі складові: обставини дії, джерело дії, об'єкт дії, спосіб дії, умова дії, мета дії. Введемо лінгвістичну зміну для кожної з складових. Опис

складових наведено у табл. 3

Таблиця 3 – Зміст структурних складових типових вимог безпеки

№	Структурні складові	Лінгвістична змінна	Питання	Зміст
1	обставини дії	$\{X\_WHERE\}$	Де? Коли?	відповідає за позначення місця та часу проведення дії
2	джерело дії	$\{X\_WHOM\}$	Ким? Чим?	визначає джерело дії
3	дія	$\{X\_ACTION\}$	Що робиться? Що зроблено?	визначає безпосередньо саму дію
4	об'єкт дії	$\{X\_OBJECT\}$	над ким? над чим?	визначає об'єкт, над яким ця дія проводиться
5	спосіб дії	$\{X\_HOW\}$	Яким чином?	визначає спосіб, в який проводиться дія
6	умова дії	$\{X\_IF\}$	За яких умов?	визначає умови, при яких дія має проводитися чи була проведена у минулому
7	мета дії	$\{X\_TARGET\}$	З якою метою?	визначає мету, з якою проводиться дія

Будь-яку вимогу безпеки можна уявити з використанням набору цих лінгвістичних змінних. Отже використання даного підходу дозволить не тільки проводити аналіз будь-якої існуючої вимоги безпеки але і генерувати іншу. Представлення твердження у формалізованому вигляді, тобто в вигляді запропонованого переліку складових, дозволяє чітко простежити місце, відповідальність, умови та мету дії, яка буде проводитись для задоволення певної вимоги безпеки.

З метою ілюстрації такого підходу зроблено аналіз (див. табл. 4) кращих практик комплексу робіт „Визначення методології життєвого циклу системи", що належить до напрямку „Життєвий цикл" процедурної області практичної діяльності (стандарт Національного інституту стандартизації та технологій США NIST SP 800-26).

Даний підхід, запропонований для аналізу існуючих вимог, також може використовуватися для формулювання нових вимог, специфічних для окремої установи. Наявність чітко визначених лінгвістичних змінних та можливість призначення їх значень дозволяє особі, що буде формулювати вимоги, визначити усі ключові моменти, які необхідно виконати для задоволення певної вимоги. Застосування даного підходу надає також можливість формування бази запитань для експертної системи [10 – 11], може бути створена за принципами, викладеними у цій статті, на основі вимог безпеки будь якого нормативного документу у сфері забезпечення безпеки інформації.

Таблиця 4 – Приклад аналізу вимог безпеки

		обставини дії	джерело дії	дія	об'єкт дії	спосіб дії	умова дії	мета дії
1	Визначення критичності системи			визначається	критичність системи			
2	Передбачення комплектом ділових документів необхідних ресурсів для адекватного забезпечення безпеки системи	у комплектах ділових документів		визначаються	необхідні ресурси			для адекватного забезпечення безпеки системи
3	Гарантування особами, що відповідають за купівлю обладнання для ІТ систем, що у	у всіх інвестиційних пропозиціях	особами, що відповідають за закупівлю ІТ	забезпечується	врахування вимог безпеки інформації			

		обставини дії	джерело дії	дія	об'єкт дії	спосіб дії	умова дії	мета дії
	будь-якій інвестиційній пропозиції враховані вимоги безпеки інформації		систем					
4	Передбачення бюджетом організації витрат на забезпечення безпеки системи з вказівкою джерел фінансування	у бюджеті організації		передбачаються	витрати на забезпечення безпеки системи	з вказівкою джерел фінансування		
5	Дозвіл вимогами існуючої документації на проведення модифікацій або закупівлю засобів захисту у випадку виявлення нових погроз та вразливостей або використання новітніх технологій		вимогами існуючої документації	дозволяється	проведення модифікацій або закупівля засобів захисту		у випадку виявлення нових погроз та вразливостей або використання новітніх технологій	

III Правила побудови вербальних відповідей-оцінок

Для формулювання вербальних відповідей-оцінок необхідно визначити правила їх побудови. Оскільки відповіді - оцінки будуються на основі типових відповідей для базових зон простору суб'єктивної логіки, то структура речення буде подібна до їх структури.

Симетричність трикутника думок відносно центра дозволяє розбити зони базових думок, а отже і типові відповіді, що відповідають їм, на три множини за принципом домінуючого параметру [8]. Таким чином маємо три множини:

- множина відповідей, що характеризують виконання процесу, що оцінюється $b \phi (d+u)$;
- множина відповідей, що характеризують невиконання процесу, що оцінюється $d \phi (b+u)$;
- множина відповідей, що характеризують невизначеність, щодо оцінки процесу, що оцінюється $u \phi (d+b)$.

Для кожної множині є три випадки співвідношення параметрів: випадок коли базовий параметр домінує цілком та два випадки домінації базового параметра та переваги одного другорядного параметру над іншим. Розглянемо правила побудови вербальних відповідей-оцінок для кожної множини окремо.

Оскільки для першої множини домінуючим параметром є довіра до виконання, базою для побудови конструкції відповідей-оцінок є „позитивне речення", для позначення якої використовується лінгвістична змінна $\{Pos\}$.

Під терміном „позитивне речення" розуміється твердження про коректне здійснення процесу.

У випадку, коли беззаперечним домінантом є ступінь виконання, як відповідь - оцінка використовується позитивне речення (рис. 6).

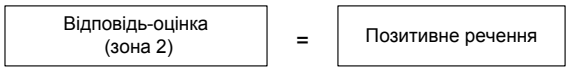


Рисунок 6 – Правило формування відповіді оцінки (зона 2)

У випадку, коли домінантом є ступінь виконання, а ступінь невиконання вимоги переважає над ступенем невизначеності, на початок позитивного речення ставиться вираз, що свідчить про виконання процесу в цілому, а на кінець додається вираз, в якому вказується на недоліки у загальному вигляді (альтернативою є внесення до бази притаманного цьому процесу недоліку) (рис. 7).

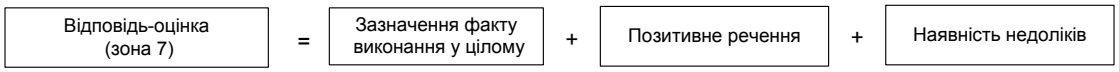


Рисунок 7 – Правило формування відповіді оцінки (зона 7)

У випадку, коли домінантом є ступінь виконання, а ступінь невизначеності переважає над ступенем невиконання вимоги, на початок позитивного речення ставиться вираз, що свідчить про виконання процесу в цілому, а на кінець додається вираз, в якому вказується, що кількість інформації не дозволяє беззаперечно стверджувати факт коректного виконання процесу (рис. 8).

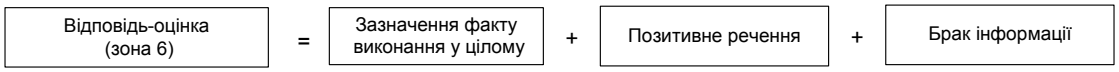


Рисунок 8 – Правило формування відповіді оцінки (зона 6)

Базою для побудови конструкції відповідей-оцінок другої множини є „заперечне речення”, для позначення якої використовується лінгвістична змінна $\{Neg\}$.

Під терміном „заперечне речення” розуміється твердження про те, що процес не виконується коректно. Для заперечного речення лінгвістична змінна $\{\text{X\_ACTION}\}$ замінюється на $\{\text{X\_ACTION\_NEG}\}$, усі інші змінні та їх значення відповідають змінним позитивного речення:

$$\text{X\_ACTION\_NEG} = \text{"}не\text{ "} + \text{X\_ACTION}. \qquad (2)$$

У випадку, коли беззаперечним домінантом є ступінь невиконання, як відповідь-оцінка використовується заперечне речення (рис. 9).

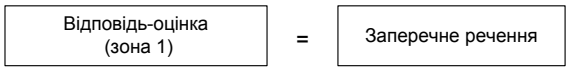


Рисунок 9 – Правило формування відповіді оцінки (зона 1)

У випадку, коли домінантом є ступінь невиконання, та ступінь виконання вимоги переважає над ступенем невизначеності: на початок заперечного речення ставиться вираз, що свідчить про те, що в ході оцінки було виявлено невиконання процесу в цілому, а на кінець додається вираз, в якому вказується, що деякі кроки в цьому напрямку все ж таки робляться (рис. 10).

Рисунок 10 – Правило формування відповіді оцінки (зона 5)

У випадку, коли домінантом є ступінь невиконання, та ступінь невизначеності переважає над ступенем виконання вимоги, на початок заперечного речення ставиться вираз, що свідчить про те, що в ході оцінки було виявлено невиконання процесу в цілому, а на кінець додається вираз, в якому вказується, що кількість інформації не дозволяє беззаперечно стверджувати, що виконання процесу здійснюється погано (рис. 11).

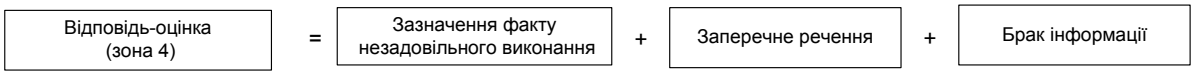


Рисунок 11 – Правило формування відповіді оцінки (зона 4)

Базою для побудови конструкції відповідей-оцінок третьої множини є „невизначене речення”, для

позначення якої використовується лінгвістична змінна $\{Ind\}$.

Під терміном „невизначене речення" розуміється твердження, яке вказує на брак інформації щодо виконання процесу. Для невизначеного речення лінгвістична змінна $\{\text{X\_ACTION}\}$ замінюється на $\{\text{X\_ACTION\_IND}\}$, усі інші змінні та їх значення відповідають змінним позитивного речення:

$$\text{X\_ACTION\_IND} = "чи\ " + \text{X\_ACTION}. \quad (3)$$

У випадку, коли беззаперечним домінантом є ступінь невизначеності, на початок невизначеного речення ставиться вираз, який свідчить про критично малу кількість інформації для прийняття будьякого рішення відносно коректності виконання процесу, що оцінюється (рис. 12).

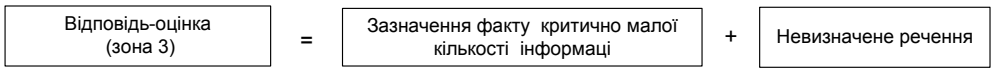


Рисунок 12 – Правило формування відповіді оцінки (зона 3)

У випадку, коли домінантом є ступінь невизначеності, та ступінь виконання вимоги переважає над ступенем невиконання, на початок невизначеного речення ставиться вираз, що свідчить про брак інформації, а на кінець додається вираз, в якому вказується на те, що деякі кроки в цьому напрямку все ж таки робляться (рис. 13).

Рисунок 13 – Правило формування відповіді оцінки (зона 5)

У випадку, коли домінантом є ступінь невизначеності, та ступінь невиконання переважає над ступенем виконання вимоги, на початок невизначеного речення ставиться вираз, що свідчить про брак інформації, а на кінець додається вираз, в якому вказується, на те, що цей процес не є практикою в установі (рис. 14).

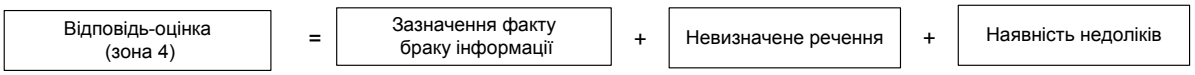


Рисунок 14 – Правило формування відповіді оцінки (зона 4)

Висновки

На сучасному етапі для проведення аудиту безпеки інформації широко використовуються національні та міжнародні стандарти. Стандартизованість такого підходу дозволяє формалізувати процес оцінки в цілому та розробити методику формування вербальних оцінок щодо зрілості процесів з забезпечення безпеки інформації. В статі наведено математичну постановку задачі вибору математичного апарату такої методики. Результатом є обґрунтування вибору апарату суб'єктивної логіки, який є дозволяє підвищити повноту оцінок, спростити процес аудиту безпеки інформації та забезпечити коректність обробки вихідних даних в умовах наявності невизначеності як наслідок швидкоплинності процесів та неповноти знань експертів.

Задача формування вербальних оцінок вирішується із застосуванням зон базових думок [8]. Визначення типової думки для певного вектору думки у просторі суб'єктивної логіки здійснюється з використанням функцій належності, які будуються для кожної зони базової думки. У методиці пропонується поєднувати зміст конкретної вимоги безпеки інформації із типовою відповіддю. Для реалізації такої можливості вимоги безпеки розкладаються на складові. Перевагою такого підходу є не тільки можливість формування вербальних оцінок зрілості процесів з забезпечення безпеки інформації в автоматизованому режимі, але і висування нових вимог безпеки.

Таким чином дана методика створює підґрунтя для створення автоматизованої системи підтримки прийняття рішення аудитора безпеки інформації, основними рисами якої є:

- орієнтованість на вимоги безпеки стандартів у галузі забезпечення безпеки інформації;
- врахування невизначеності, яка виникає в аудитора в ході проведення оцінки, шляхом застосування математичного апарату суб'єктивної логіки;
- надання відповідей та одержання оцінок у вербальному вигляді, який є більш зручним для сприйняття людиною.

*Література: **1**. NIST SP 800-53 Marianne Swanson, Nadya Bartol et al. Security Metrics Guide for Information Technology Systems. 2003. **2**. 2. Марка Д. А., МакГоуэл К. М. Методология структурного анализа и проектирования SADT. - М.: Метатехнология, 1993. - 240 с. **3**. A. Jøsang., S. J. Knapskog. A Metric for Trusted Systems. In Reinhard Posh, editor, Proceedings of the 15th IFIP/SEC International Information Security Conference. IFIP, 1998 **4**. A. Jøsang An Algebra for Assessing Trust in Certification Chains. In J. Kochmar, editor, Proceedings of the Network and Distributed Systems Security Symposium (NDSS'99). The Internet Society, 1999. **5**. Леншин А. В. Применение аппарата субъективной логики для оценки безопасности банковских ИТ-систем // Актуальні проблеми та перспективи розвитку фінансово-кредитної системи України: Збірник наукових статей. Харків: Фінарт, 2002, с. 410 – 412. **6**. Леншин А. В., Потий А. В. Применение оператора попарной усредненной конъюнкции для оценки уровня защищенности ИТ-систем // Збірник наукових статей за матеріалами VI міжнародної науково практичної конференції "Безпека інформації в інформаційно-телекомунікаційних системах", - Київ, 2003, с 57 – 58. 7. Потий А. В., Леншин А. В. Оценка защищенности информационно-телекоммуникационных систем с использованием математического аппарата субъективной логики //7-я Научно - практическая конференция «Безопасность информации в информационно – телекоммуникационных системах», Киев. 2004 р. **8**. Потій О.В., Лєншин А.В. Методика визначення думок експертів відносно зрілості безпеки інформації із застосуванням математичного апарату суб'єктивної логіки //Науково-технічний збірник „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 9, Київ, 2004 р., с. 38-47. **9**. Потій О. В., Лєншин А. В. Основні положення математичного апарату суб'єктивної логіки та його застосування для оцінки рівня зрілості систем забезпечення безпеки інформації //Радиотехника. Тематический выпуск "Информационная безопасность", вып. 141, Харьков, 2005 г., с. 144-160. **10.** Потий А. В., Леншин А. В. Принципы построения системы экспертной оценки защищенности ИТ-систем «Советник» //Збірник наукових статей за матеріалами VI міжнародної науково практичної конференції "Безпека інформації в інформаційно-телекомунікаційних системах",.- Київ, 2003, с 25-26. **11.** Лєншин А. В., Потій О. В. Практичні рекомендації по використанню системи "Радник" при оцінці рівня організаційного захисту інформації в ІТС //VII Научно - практическая конференция «Безопасность информации в информационно – телекоммуникационных системах», Киев. 2004 р.*

УДК 681.3.06

СИСТЕМНИЙ ПІДХІД ДО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ДЕРЖАВНОЇ ТАЄМНИЦІ

Олександр Архипов, Валерій Ворожко*

Національний технічний університет України „КПІ", Національна академія СЕ України

Анотація: **Розглядається застосування методології керування інформаційними ризиками для аналізу ефективності систем захисту державної таємниці.**

Summary: **Considered application of risk-management methodology for research on the state secret protection.**

Ключові слова: **Інформаційний ризик, державна таємниця, захист інформації.**

І Вступ

Державна таємниця (ДТ) - специфічна категорія таємних відомостей, умови віднесення інформації до якої та захист цієї інформації здійснюється відповідно до закону [1]. Процес глобальної інформатизації суспільства, що зараз триває, приніс для ДТ, як і для інших видів інформації з обмеженим доступом (ІзОД) певні проблеми, пов'язані із особливостями захисту ДТ в умовах нового інформаційного середовища. Вперше ці проблеми окреслилися наприкінці 60-х - на початку 70-х років двадцятого століття, а особливої актуальності набули в останні десять років через масоване впровадження в різних сферах діяльності сучасних інформаційних технологій.

За цей час техніка та методологія захисту інформації, пройшли довгий шлях розвитку – від окремих розрізнених нескладних механізмів захисту до системної концепції захисту, втіленням якої є цілеспрямоване використання комплексу організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів захисту інформації. Суть системної концепції - поєднання у найбільш раціональний спосіб усіх наведених вище заходів в певній організаційній формі - системі захисту інформації (СЗІ). Наскільки вдалим є це поєднання, як визначити рівень успішності функціонування СЗІ? Ці цілком природні в загальному випадку питання набувають особливої актуальності в разі, коли об'єктом захисту є ДТ, рівень важливості й,