РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО КІЛЬКІСНОГО ОЦІНЮВАННЯ РІВНЯ РЕАЛІЗАЦІЇ ВИМОГ СТАНДАРТУ ISO/IEC 27001:2022

Добринін І.С., Пашкова А.В.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна.

E-mail: ihor.dobrynin@nure.ua,
anhelina.pashkova@nure.ua

Abstract

In the modern world, information security is a key aspect for companies, confirmed by the implementation of information security management systems. The audit of these systems is an integral stage. ISO/IEC 27001 and other standards provide certain frameworks for this procedure. However, most standards are declarative or imperative in nature and do not contain specific proposals for assessing the audit results. This work proposes an approach to the quantitative assessment of the implementation of the ISO/IEC 27001:2022 standard by decomposition the audit into specific criteria. For a clear display of the adoption rate of a certain criterion, a fan chart was used, where the levels of implementation of each subprocesses was indicated.

У сучасному світі, інформаційна безпека підприємств набула великого значення. Це обумовлює розробку та впровадження систем управління інформаційною безпекою (СУІБ), які функціонують відповідно до циклу Демінга-Шухарта. Зазначений підхід визначає модель безперервного поліпшення процесів будь-яких систем управління на етапах планування, функціонування, перевірки та впливу (дій).

Одним із найважливіших етапів роботи систем управління інформаційною безпекою є проведення аудиту стану цієї системи. Питанням вимог та реалізації процедури аудиту інформаційної безпеки присвячена низька стандартів, зокрема ISO/IEC 27001, ISO/IEC 27007, NIST SP 500-38, CIP-006, ITAF та інші. Проте, проведений авторами аналіз відомих стандартів показав, що вони, як правило, мають або декларативний або імперативний характер та не містять конкретних пропозицій щодо оцінювання результатів аудиту елементів СУІБ.

Метою цієї роботи є розробка пропозицій щодо кількісного оцінювання рівня реалізації вимог стандарту ISO/IEC 27001:2022.

Запропонований підхід полягає в том, що кожен критерій аудиту, зазначений у стандарті ISO/IEC 27001:2022 [1] може бути представлений як сукупність часткових критеріїв. Таким чином, підсумковий результат визначення рівня впровадження конкретного критерію (К) може бути визначений за допомогою виразу:

$$K = \sum_{i=1}^{n} k_i, \tag{1}$$

де n – кількість часткових критеріїв;

k_i – значення і-го часткового критерія.

Визначимо часткові критерії k_i через рівень їхнього впровадження (реалізації) та коефіцієнт значущості:

$$k_i = \mu_i \cdot \beta_i, \quad 1 \le i \le n, \tag{2}$$

де μ_i – рівень впровадження (реалізації) і-го часткового критерія,

β_i – коефіцієнт значущості і-го часткового критерія, який визначається на основі експертної інформації отриманої від групи аудиторів.

З метою нормування розрахунків, вважатимемо, що адитивна сукупність значень β_i дорівнює одиниці, тобто:

$$\sum_{i=1}^{n} \beta_i = 1. \quad (3)$$

Для визначення рівня впровадження (реалізації) і-го часткового критерія (μ_i) пропонується наступний підхід:

$$\underset{1 \le i \le n}{\mu_i} = \begin{cases} 1 & \forall \ A, \\ 0{,}75 & \forall \ B, \\ 0{,}5 & \forall \ C, \\ 0{,}25 & \forall \ D, \\ 0 & \forall \ E. \end{cases} \quad (4)$$

Під час оцінювання рівня впровадження і-го часткового критерія вважатимемо, що:

- елемент A відповідає такому стану часткового критерію, при якому цей критерій визначений, впроваджений, систематично переглядається та його реалізація може бути рекомендована як зразок кращих практик (відмінно);
- елемент B відповідає такому стану часткового критерію, при якому цей критерій визначений, впроваджений, систематично переглядається та але його реалізація є найактуальнішою для конкретної організації проте не може бути рекомендована як зразок кращих практик (майже відмінно);
- елемент C відповідає такому стану часткового критерію, при якому цей критерій визначений, впроваджений, переглядається, але його реалізація має певні недоліки або частковий критерій впроваджений із незначними зауваженнями (добре);
- елемент D відповідає такому стану часткового критерію, при якому цей частковий критерій розглядається в організації, але має суттєві недоліки щодо його визначення або впровадження (задовільно);
- елемент E відповідає такому стану часткового критерію, при якому цей критерій або не визначений та/або не впроваджений (не задовільно).

Отже, відповідно до запропонованого підходу, для кількісного оцінювання рівня реалізації вимог стандарту ISO/IEC 27001:2022 (конкретного критерію – K) доцільно сформувати матрицю розрахунку, загальний вигляд якої надано в таблиці 1.

Таблиця 1. Розрахунок рівня впровадження конкретного критерія СУІБ

Частковий показник	Оцінка часткового показника	Коефіцієнт значущості	Розрахунок часткового показника
Частковий показник 1	$\mu_1 = f(A_1 v B_1 v C_1 v D_1 v E_1)$	β_1	$k_1 = \mu_1 \cdot \beta_1$
Частковий показник 2	$\mu_2 = f(A_2 v B_2 v C_2 v D_2 v E_2)$	β_2	$k_2 = \mu_2 \cdot \beta_2$
…	…	…	…
Частковий показник n	$\mu_n = f(A_n v B_n v C_n v D_n v E_n)$	β_n	$k_n = \mu_n \cdot \beta_n$
Підсумковий результат рівня впровадження конкретного критерію			$K = \sum_{i=1}^{n} k_i$

Зазначений підхід був апробований для отримання оцінки рівня впровадження вимог стандарту ISO/IEC 27001:2022 доступу до фізичних об’єктів.

Так, відповідно до вище наданого, процес доступу до фізичних об’єктів (критерій К) можна розглядати як сукупність підпроцесів (часткових критеріїв), які підлягають оцінюванню. Відповідно до ISO/IEC 27001:2022, до основних з них можна віднести: периметр фізичної безпеки; порядок доступу осіб до фізичних об’єктів; убезпечення офісів, кімнат та обладнання; порядок роботи в зонах безпеки; зони доставки та відвантаження; оптимізація розміщення засобів захисту обладнання; порядок обслуговування обладнання; порядок безпечного вилучення або повторного використання обладнання; резервування обладнання на випадок стихійних лих, тощо.

Зазначимо, що перелік підпроцесів безпосередньо залежить від організації, яка підлягає аудиту та може змінюватися відповідно до цілей та критеріїв аудиту.

Приклад оцінювання стану підпроцесу «Периметр фізичної безпеки» надано на рис. 1.

Вимога		Структура організації						
	Частковий показник	Оцінка часткового показника					Коефіцієнт значущості	Розраховане значення часткового показника
		A	B	C	D	E		
1	Чи розміщений чітко периметр	1					0,1	0,1
2	Чи є фізичні бар'єри на території об'єкту			1			0,1	0,05
3	Чи надійна та безпека конструкція під час стихійних лих			1			0,2	0,1
4	Чи обладнані пожежні двері				1		0,1	0,025
5	Чи присутня система виявлення порушників		1				0,1	0,075
6	Чи відокремлені засоби оброблення інформації				1		0,1	0,025
7	Чи впроваджене обмеження доступу без супроводу			1			0,1	0,05
8	Чи найнята безперервна охорона в вибраних точках фізичного доступу (особливо в місцях без відеоспостереження)			1			0,1	0,05
9	Чи впроваджені вестибюлі контролю доступу					1	0,1	0
Результат впровадження		0,475						

Рис. 1. Варіант аналізу розрахунку результату впровадження процесу «Периметр фізичної безпеки»

Для наочного відображення рівня впровадження певного критерія (у нашому прикладі – доступ до фізичних об’єктів) доцільно використовувати віялову (або звичайну) діаграму на якій зазначаються рівні впровадження кожного з підпроцесів (часткових критеріїв), як це показано на рис. 2.

№	Вимога	Розрахований показник рівня впровадження
1	Периметр фізичної безпеки	0,475
2	Заходи безпеки фізичного прибуття	0,575
3	Убезпечення офісів, кімнат та обладнання	0,825
4	Робота в зонах безпеки	0,625
5	Зони доставки та відвантаження	0,9
6	Розміщення та захист обладнання	0,65
7	Допоміжні комунальні служби	0,6875
8	Безпека кабельних мереж	0,425
9	Обслуговування обладнання	0,5875
10	Переміщення майна	0,8125
11	Безпека обладнання та ресурсів СУБ поза службовими приміщеннями	0,825
12	Безпечне вилучення або повторне використання обладнання	0,75
13	Обладнання користувачів, залишене без нагляду	0,8375
14	Політика чистого стола та чистого екрана	0,8375
15	Альтернативне робоче місце	0,775
	Загальний рівень впровадження вимог стандарту	0,705833333

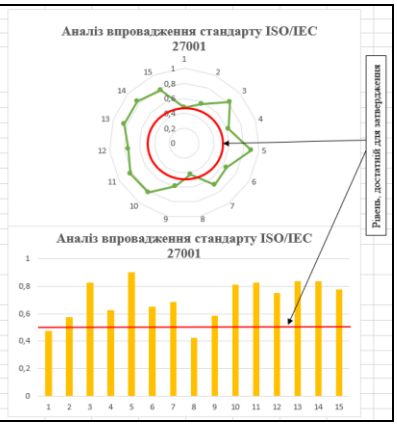

Рис. 2. Варіант оцінки рівня впровадження вимог стандарту ISO/IEC 27001:2022 доступу до фізичних об’єктів

Отже, у роботі надані пропозиції щодо кількісного оцінювання рівня реалізації вимог стандарту ISO/IEC 27001:2022. Запропоновані рішення не суперечать раніш відомим підходам отримання оцінки за результатами аудиту, проте надають методологічну основу кількісного оцінювання критеріїв аудиту.

Література

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. URL: https://www.iso.org/ru/standard/27001 (дата звернення: 07.11.2023).

2. Пашкова А. В. Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій. *Аналіз наявних методів аудиту фізичних об’єктів та безпеки інфраструктури* : матеріали 27-го Міжнародного молодіжного форуму м. Харків 10 – 12 травня 2023 р., Харків, 2023. С. 66 – 67.

3. Добринін І. С. Вдосконалення методики факторного аналізу інформаційних ризиків / І. С. Добринін, Н. О. Мальцева // Системи обробки інформації. – 2017. – № 3(149). – С. 146-150.

4. ITAF Information Technology Assurance Framework. URL: http://www.isaca.org.ua/index.php/standards/itaf (дата звернення: 07.11.2023).