УДК 004.056:005.33 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.081

ПРОПОЗИЦІЇ ЩОДО ОЦІНЮВАННЯ КОМПЕТЕНТНОСТІ АУДИТОРІВ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЇНОЮ БЕЗПЕКОЮ

Пашкова А.В., Вакуленко Д.В.
Науковий керівник – доцент каф. ІКІ ім. В.В. Поповського Добринін І.С.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського, м. Харків, Україна
e-mail: anhelina.pashkova@nure.ua, danyil.vakulenko@nure.ua.

The work is devoted to the actual problem of assessing the consistency of experts' opinions in the field of information security. The work provides proposals for assessing the agreement of experts' opinions using the concordance coefficient, which takes into account the ranking of factors and provides a more accurate assessment of agreement than other methods.

Проведення аудитів – це важлива частина при побудові систем управління інформаційною безпекою (СУІБ). Відповідно до [1], для проведення аудитів організація повинна призначити групу аудиторів, на яких, серед інших задач, покладатиметься задача формування підсумкової оцінки стану інформаційної безпеки.

У роботі [2] надані пропозиції щодо кількісного оцінювання рівня реалізації вимог стандарту ISO/IEC 27001:2022. Зазначимо, що оцінювання відбувається на основі експертної інформації отриманої від аудиторів, які, у цьому випадку, виконують роль експертів.

Відповідно до теорії прийняття рішень [3] експертне оцінювання передбачає рішення п’яти основних задач.

1) Формування групи потенційних експертів.
2) Оцінювання компетентності кожного з експертів.
3) Розрахунок репрезентативності групи експертів.
4) Оцінювання узгодженості думок експертів.
5) Формування експертного висновку.

Проведений авторами аналіз основних етапів експертного оцінювання показує, що одним із найскладніших моментів є оцінювання компетентності кожного з експертів.

У літературі [1] надана формула, за допомогою якої можна оцінити компетентність експертів:

$$K_{K_i} = \frac{K_{a_i} + K_{o_i}}{K_{a_{max}} + K_{o_{max}}}, \quad (1)$$

де K_{a_i} – коефіцієнт аргументації і-го експерта;

K_{o_i} – коефіцієнт обізнаності і-го експерта;

$K_{a_{max}}$, $K_{o_{max}}$ – максимально можливі оцінки аргументації та обізнаності експертів.

Зазвичай, під час розрахунків приймають $K_{a_{max}} = 1, K_{o_{max}} = 1$.

Аналіз виразу (1) показує, що компетентність і-го експерту (K_{K_i}) є функцією двох величин: коефіцієнтів аргументації (K_{a_i}) та обізнаності (K_{o_i}). Причому, ці величини (K_{a_i} та K_{o_i}) мають однаковий вплив на підсумкову оцінку. Це, на нашу думку, призводить до викривлення підсумкової оцінки компетентності. Так, наприклад, якщо перший експерт максимально аргументований ($K_{a_1} \to max$) , але необізнаний ($K_{o_1} \to 0$), а другий експерт – не аргументований ($K_{a_2} \to 0$), але максимально обізнаний ($K_{o_1} \to max$), то в цьому випадку підсумкова оцінка компетенції є однаковою, що суперечить логіці.

Тому авторами даної роботи пропонується наступний підхід для вирішення зазначеної колізії. А саме:

– встановлення порогового рівня аргументації експертів, який дозволяє виконувати задачу з формування експертного оцінювання ($K_{a_{\text{порог}}}$);

– використання вагового коефіцієнту ω_j $(j = 1 \dots N)$, який враховує обізнаність і-го експерта за j-ю областю оцінювання (документація, мережна безпека, фізичний доступ тощо).

У цьому випадку, формула (1) матиме вигляд:

$$K_{K_i} = \sum_{j=1}^{N} \frac{K_{a_i} + \omega_j \cdot K_{o_i}}{K_{a_{max}} + K_{o_{max}}} \quad \forall\, K_{a_i} \geq K_{a_{\text{порог}}} \qquad (2)$$

Зазначимо, що визначення порогового рівня аргументації експертів та вагових коефіцієнтів ω_j покладається на особу, яка керує програмою аудиту.

Таким чином, завдяки запропонованому підходу, можна запобігти викривленій оцінці компетентності експертів (аудиторів) СУІБ на етапі формування групи з аудиту.

Список використаних джерел:

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements : вебсайт. URL: https://www.iso.org/standard/27001 (дата звернення: 28.02.2024).

2. Добринін І. С., Пашкова А. В. Розробка пропозицій щодо кількісного оцінювання рівня реалізації вимог стандарту ISO/IEC 27001:2022. *Міжнародна науково-технічна конференція «Інформаційно-комунікаційні технології та кібербезпека (ІКТК-2023)»*. Харків, 2023. URL: https://ice.nure.ua/wp-content/uploads/2024/01/43_Dobrynin-I.S.-Pashkova-A.V._Str.151-153.pdf (дата звернення 28.02.2024).

3. Файнзільберг Л. С., Жукова О. А., Якимчук В. С. Теорія прийняття рішень : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2018. 250 с.