КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1179
УДК 004.056:005.963

Запорожченко Михайло Михайлович
доктор філософії
доцент кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0003-0182-9497
m.zaporozhchenko@duikt.edu.ua

Легомінова Світлана Володимирівна
доктор економічних наук, професор
завідувач кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-4433-5123
s.legominova@duikt.edu.ua

Рабчун Дмитро Ігорович
кандидат технічних наук
доцент кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-5555-0910
d.rabchun@duikt.edu.ua

ФОРМАЛІЗАЦІЯ СИСТЕМИ ПОКАЗНИКІВ ОЦІНЮВАННЯ РЕЗУЛЬТАТИВНОСТІ ПРОГРАМ НАВЧАННЯ ПЕРСОНАЛУ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. У статті розглянуто проблему формалізації системи показників оцінювання результативності програм навчання персоналу. Актуальність дослідження зумовлена тим, що в практиці організаційного забезпечення безпеки оцінювання таких програм часто зводиться до використання окремих фрагментарних характеристик, зокрема охоплення навчанням, результатів тестування або періодичності проведення занять, що не забезпечує цілісного кількісного подання фактичної результативності програми. Це ускладнює порівняння програм між собою, аналіз динаміки їх розвитку та обґрунтування управлінських рішень щодо вдосконалення навчального процесу. Метою статті є формалізація системи показників оцінювання результативності програм навчання персоналу шляхом визначення складу кількісних індикаторів, обґрунтування їх формального подання та побудови інтегральної оцінки. У роботі запропоновано систему з шести взаємопов'язаних показників, що охоплюють основні аспекти результативності програм навчання персоналу, а саме: охоплення навчанням, покриття релевантних тематичних блоків, результат підсумкового тестування, актуалізацію програми, поведінкову результативність та своєчасність повторного навчання. Для кожного показника наведено формальний вираз, що забезпечує можливість його кількісного визначення в межах єдиної моделі оцінювання. Обґрунтовано доцільність використання ентропійного методу для визначення вагових коефіцієнтів показників, що дозволяє враховувати їх відносну дискримінативну здатність на множині фактичних або змодельованих спостережень. Для демонстрації методики в роботі сформовано сценарно-аналітичну модель на основі характерних діапазонів значень показників для програм навчання різного рівня зрілості. Наукова новизна дослідження полягає у формалізації системи показників оцінювання результативності програм навчання персоналу та в обґрунтуванні підходу до побудови інтегрального показника на основі ентропійно визначених вагових коефіцієнтів. Отримані результати показали, що найбільший внесок у диференціацію програм навчання за рівнем результативності забезпечують показники поведінкової результативності, своєчасності повторного навчання та покриття релевантних тематичних блоків. Практичне значення дослідження полягає в можливості використання запропонованої моделі для порівняльного аналізу програм навчання, оцінювання динаміки їх результативності та підтримки рішень щодо вдосконалення навчального процесу.

© М. М. Запорожченко, С. В. Легомінова, Д. І. Рабчун, 2026

Ключові слова: кібербезпека; інформаційна безпека; управління інформаційною безпекою; навчання персоналу; оцінювання результативності; система показників; ентропійний метод; моделювання.

ВСТУП

Навчання персоналу з інформаційної безпеки є одним із ключових організаційних засобів підтримання належного рівня безпеки в організації, оскільки його результативність визначає не лише рівень ознайомлення працівників із встановленими вимогами та правилами безпечної поведінки, але й здатність коректно діяти в умовах інцидентів, дотримуватися внутрішніх процедур і зберігати актуальність знань. У практиці організаційного забезпечення інформаційної безпеки оцінювання програм навчання персоналу здебільшого зводиться до окремих фрагментарних характеристик, зокрема охоплення навчанням, частоти проведення занять або результатів підсумкового тестування [1]. У дослідженнях, присвячених навчанню з кібербезпеки, підкреслюється, що орієнтація лише на формальне проходження навчальних заходів або на виконання мінімальних вимог не дає підстав вважати, що відбулося реальне покращення безпечної поведінки персоналу [2].

У сучасних підходах до побудови програм навчання персоналу навчальний процес розглядається як керований циклічний механізм, що охоплює планування, реалізацію, оцінювання та подальше оновлення змісту відповідно до змін профілю загроз, внутрішніх процедур і функціональних потреб організації [3, 4]. За таких умов відсутність формалізованої системи показників ускладнює не лише оцінювання окремої програми, але й порівняння різних програм між собою, моніторинг їх результативності в часі та використання відповідних оцінок у ширших задачах аналізу стану інформаційної безпеки. Це зумовлює потребу у формалізації системи показників, яка б забезпечувала кількісне, структуроване та методично узгоджене оцінювання результативності програм навчання персоналу з інформаційної безпеки.

Постановка проблеми. Наявні підходи до оцінювання програм навчання персоналу з інформаційної безпеки переважно орієнтовані на окремі процесні або контрольні характеристики та не забезпечують їх інтегрованого використання в межах єдиної системи оцінювання. Унаслідок цього результативність навчання описується фрагментарно, а отримані значення не мають достатньої аналітичної придатності для обґрунтування рішень щодо вдосконалення програм навчання. Особливої уваги потребує те, що різні аспекти результативності, зокрема охоплення персоналу, покриття релевантних тематичних блоків, рівень засвоєння матеріалу, своєчасність актуалізації програми, поведінкова результативність у симуляційних сценаріях та повторність навчання, мають різну природу й потребують узгодженого подання в межах єдиної моделі.

Отже, науково-методична проблема полягає у відсутності формалізованої системи показників, яка б дозволяла визначити релевантний склад індикаторів результативності програм навчання персоналу з інформаційної безпеки, забезпечити їх зіставність у межах єдиної шкали, обґрунтувати спосіб визначення вагових коефіцієнтів і побудувати інтегральний показник, придатний для подальшого аналітичного використання.

Аналіз останніх досліджень і публікацій. Проблема оцінювання результативності програм навчання персоналу з інформаційної безпеки висвітлюється в літературі переважно фрагментарно. Робота [5] зосереджена на побудові програм навчання й обізнаності для малих і середніх організацій, в роботі [2] обґрунтовано обмеженість комплаєнс-орієнтованого підходу до навчання, а в [6] автори дослідили фактори організаційного прийняття комп’ютеризованих інструментів навчання. У цих працях увагу приділено організації програм, їх упровадженню та прийняттю, однак питання побудови цілісної кількісної системи оцінювання результативності програм навчання не розв’язано.

Подальші дослідження змістили акцент на метрики та прикладні рамки оцінювання. В роботі [7] автори показали відсутність усталеного набору метрик для оцінювання програм навчання з кібербезпеки. В [8] було запропоновано рамкову структуру навчання та оцінювання для дистанційних працівників, а в [9] продемонстровано значущість поведінкових метрик у фішингових симуляціях і неоднорідність результатів між бізнес-підрозділами. Разом з тим ці роботи або зосереджені на окремих групах показників, або мають рамковий характер і не переходять до інтегральної моделі результативності програм навчання.

У роботі [10] автори показали методичну неоднорідність сучасних підходів до навчання з кібербезпеки, а в роботі [11] встановили, що програми навчання дають відчутніші результати для знань, ставлень і намірів, ніж для фактичної поведінки. Це підтверджує, що оцінювання результативності не може зводитися до окремих тестових або процесних характеристик.

Отже, незважаючи на наявність значної кількості праць, присвячених окремим аспектам навчання персоналу з інформаційної безпеки, у літературі відсутній цілісний формалізований підхід до оцінювання результативності програм навчання. Недостатньо опрацьованими залишаються питання системного поєднання різнорідних показників, визначення їх відносної значущості та побудови інтегральної оцінки, придатної для подальшого аналітичного використання.

Метою статті є формалізація системи показників оцінювання результативності програм навчання персоналу з інформаційної безпеки шляхом визначення складу кількісних індикаторів, обґрунтування їх формального подання та побудови інтегральної оцінки результативності.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Результативність програм навчання персоналу доцільно розглядати як багатовимірну характеристику, що відображає охоплення персоналу навчанням, повноту змістового наповнення програми, рівень засвоєння навчального матеріалу, своєчасність актуалізації навчального контенту, поведінковий ефект навчання та безперервність підтримання актуальних знань у часі. За такого підходу оцінювання не може ґрунтуватися на одному показнику, оскільки кожен індикатор відображає лише окремий аспект функціонування програми.

З урахуванням зазначеного систему показників результативності програм навчання персоналу пропонується задати множиною:

$$T = \{t_1, t_2, t_3, t_4, t_5, t_6\}, \tag{1}$$

де t_1 – охоплення персоналу навчанням; t_2 – покриття програмою релевантних тематичних блоків; t_3 – результат підсумкового тестування; t_4 – актуалізація програми навчання; t_5 – поведінкова результативність; t_6 – своєчасність повторного навчання.

Запропонована система показників може застосовуватися як на рівні організації в цілому, так і на рівні окремих підрозділів або функціонально однорідних груп персоналу.

Такий підхід є доцільним, оскільки для різних організаційних одиниць можуть бути релевантними різні тематичні блоки навчання, різні сценарії контрольних перевірок і різні вимоги до підтримання актуальності знань.

У разі диференційованого оцінювання для кожного підрозділу формується власний набір значень показників $T^{(d)} = \left\{t_1^{(d)}, t_2^{(d)}, t_3^{(d)}, t_4^{(d)}, t_5^{(d)}, t_6^{(d)}\right\}$, а інтегральна оцінка на рівні організації визначається подальшим агрегуванням часткових оцінок.

Показники результативності програм навчання персоналу визначаються таким чином:

$$t_1 = \frac{N_{tr}}{N_{req}}, \tag{2}$$

де N_{tr} – кількість працівників, які пройшли навчання в межах оцінюваного періоду; N_{req} – кількість працівників, для яких проходження навчання було обов’язковим;

$$t_2 = \frac{N_{cov}^{rel}}{N_{rel}}, \tag{3}$$

де N_{rel} – кількість релевантних тематичних блоків програми навчання для оцінюваної організаційної одиниці; N_{cov}^{rel} – кількість таких блоків, фактично охоплених програмою;

$$t_3 = \frac{1}{N_{test}} \sum_{i=1}^{N_{test}} \frac{S_i}{S_{max}}, \tag{4}$$

де N_{test} – кількість працівників, які проходили підсумкове тестування; S_i – результат i-го працівника; S_{max} – максимально можливий тестовий бал;

$$t_4 = \frac{N_{upd}^{timely}}{N_{upd}^{req}}, \tag{5}$$

де N_{upd}^{req} – кількість випадків, у яких оновлення програми навчання було необхідним унаслідок інцидентів або релевантних змін профілю загроз, внутрішніх процедур або вимог до безпечної поведінки; N_{upd}^{timely} – кількість таких випадків, у яких оновлення було виконане в межах установленого строку;

$$t_5 = \frac{N_{corr}}{N_{sim}}, \tag{6}$$

де N_{sim} – кількість працівників, які брали участь у симуляційних сценаріях; N_{corr} – кількість працівників, дії яких визнано коректними відповідно до встановлених критеріїв реагування;

$$t_6 = \frac{N_{ret}^{timely}}{N_{ret}^{req}}, \tag{7}$$

де N_{ret}^{req} – кількість працівників, для яких повторне навчання було обов'язковим у межах оцінюваного періоду; N_{ret}^{timely} – кількість працівників, які пройшли повторне навчання у встановлений строк.

Запропонований набір показників дозволяє розмежувати основні аспекти результативності програми навчання. Показник t_1 характеризує фактичне персоналу навчанням, t_2 – повноту змістового покриття програми, t_3 – рівень засвоєння навчального матеріалу, t_4 – своєчасність актуалізації змісту, t_5 – поведінковий ефект навчання в умовах контрольованих сценаріїв, а t_6 – безперервність підтримання актуальних знань у персоналу.

Формування сценарного простору оцінювання результативності програми. Для визначення вагових коефіцієнтів показників результативності програм навчання персоналу може бути використано два підходи. За наявності достатнього масиву внутрішніх даних організації ентропійний аналіз доцільно виконувати безпосередньо на фактичних значеннях показників, зокрема на рівні окремих підрозділів або функціонально однорідних груп персоналу.

У такому випадку множина спостережень формується з реальних значень $t_1, \dots, t_6$, а вагові коефіцієнти визначаються на основі фактичної варіативності показників у межах організації. Якщо повна та зіставна внутрішня база даних відсутня, для демонстрації методики та побудови множини спостережень використовується сценарно-аналітичний підхід.

У межах цього підходу простір оцінювання формується на основі чотирирівневої шкали зрілості програм навчання персоналу, узгодженої з CSF Tiers NIST CSF 2.0: частковий, ризик-орієнтований, повторюваний та адаптивний рівні [12]. Оскільки зазначена шкала задає якісну прогресію впорядкованості та зрілості практик, а не жорсткі числові межі, її кількісне подання виконується через характерні діапазони значень окремих показників.

Сценарний простір задається множиною $S = \{S_1, S_2, \dots, S_m\}$, де кожен сценарій S_s описується вектором значень показників результативності програми навчання: $S_s = \{t_{s1}, t_{s2}, t_{s3}, t_{s4}, t_{s5}, t_{s6}\}$, $t_{sj} \in [0; 1]$. Оскільки всі показники $t_1, \dots, t_6$ подані у відносній формі та належать інтервалу $[0; 1]$, подальше моделювання виконується безпосередньо для величин t_{sj} без додаткової нормалізації.

Для кожного показника t_j і кожного рівня зрілості L_k, $k = 1, \dots, 4$ задається характерний діапазон значень $U_{jk} = [\alpha_{jk}; \beta_{jk}]$, де α_{jk} та β_{jk} є відповідно нижньою та верхньою межами типових значень j-го показника для k-го рівня зрілості. На відміну від жорстких класифікаційних меж, зазначені діапазони можуть частково перекриватися. Таке перекриття відображає поступовий характер переходу між рівнями зрілості програм навчання та не допускає їх спрощеного дискретного розмежування за одним показником.

Отже, наведені інтервали не мають нормативного характеру й використовуються як аналітичне подання типових значень показників для програм різного рівня зрілості.

У загальному вигляді значення j-го показника в s-му сценарії формується як реалізація в межах діапазону, характерного для відповідного рівня зрілості: $t_{sj} \in [\alpha_{jk}; \beta_{jk}]$, якщо $S_s \in L_k$. За такого підходу варіативність сценаріїв забезпечується самими діапазонами значень показників, тому введення додаткових відхилень не є обов'язковим. Це спрощує інтерпретацію моделі та зменшує її залежність від

допоміжних параметрів. Характерні діапазони значень показників, наведені в табл. 1, сформовано як експертно-аналітичну інтерпретацію якісної прогресії рівнів зрілості.

Таблиця 1

Характерні діапазони значень показників результативності програм навчання персоналу за рівнями зрілості

Рівень	t_1	t_2	t_3	t_4	t_5	t_6
L_1	[0.00; 0.50]	[0.00; 0.20]	[0.00; 0.35]	[0.00; 0.20]	[0.00; 0.10]	[0.00; 0.20]
L_2	[0.20; 0.70]	[0.10; 0.50]	[0.20; 0.60]	[0.15; 0.50]	[0.05; 0.30]	[0.10; 0.30]
L_3	[0.50; 0.85]	[0.50; 0.80]	[0.55; 0.85]	[0.45; 0.80]	[0.25; 0.65]	[0.30; 0.70]
L_4	[0.75; 1.00]	[0.75; 1.00]	[0.80; 1.00]	[0.70; 1.00]	[0.60; 1.00]	[0.60; 1.00]

Їх побудова спирається на сучасні підходи до оцінки зрілості у сфері інформаційної безпеки та навчання з кібербезпеки, згідно з якими нижчі рівні пов'язуються з фрагментарними та нерегулярними практиками, тоді як вищі – із повторюваністю, системністю, актуалізацією та стійкішим поведінковим ефектом [10, 13-17].

Отже, наведені межі не мають нормативного характеру, а використовуються як формалізоване подання типових значень показників для програм навчання різного рівня зрілості. У разі наявності достатніх внутрішніх даних організації ентропійний аналіз виконується безпосередньо на фактичних значеннях показників, сформованих для підрозділів, функціональних груп або окремих програм навчання. За відсутності такої бази сценарний простір використовується як засіб формалізованого подання множини спостережень для подальшого визначення вагових коефіцієнтів показників.

Визначення вагових коефіцієнтів показників. Наступним етапом після формування множини спостережень є визначення вагових коефіцієнтів показників $t_1, \dots, t_6$. Оскільки окремі показники можуть мати різну варіативність у межах досліджуваної сукупності, їх агрегування доцільно здійснювати з урахуванням дискримінативної здатності кожного показника. Для цього використано ентропійний метод, який дозволяє визначати вагові коефіцієнти на основі структури розподілу значень показників у множині спостережень. Нехай множина спостережень містить m елементів, кожен із яких характеризується значеннями показників $t_1, \dots, t_6$. У такому разі формується матриця:

$$T = \begin{bmatrix} t_{11} & t_{12} & \cdots & t_{16} \\ t_{21} & t_{22} & \cdots & t_{26} \\ \vdots & \vdots & \ddots & \vdots \\ t_{m1} & t_{m2} & \cdots & t_{m6} \end{bmatrix}, \tag{8}$$

де t_{sj} – значення j-го показника для s-го спостереження. Як спостереження можуть розглядатися окремі підрозділи, функціональні групи персоналу або сценарії, сформовані в межах сценарно-аналітичного підходу. Для кожного показника обчислюються відносні частки $q_{sj} = \frac{t_{sj}}{\sum_{s=1}^{m} t_{sj}}$, які характеризують внесок -го спостереження у загальний розподіл значень j-го показника. На основі цих величин визначається нормалізована ентропія Шеннона [18]:

$$E_j = -\frac{1}{\ln m} \sum_{s=1}^{m} q_{sj} \ln q_{sj}, \tag{9}$$

де $E_j \in [0; 1]$ – ентропійна оцінка -го показника.

Чим ближче значення E_j до одиниці, тим меншою є варіативність відповідного показника в межах досліджуваної множини, а отже, тим меншою є його здатність диференціювати програм навчання за рівнем результативності. Менші значення ентропії, навпаки, відповідають вищій неоднорідності розподілу показника та більшій інформативності щодо розрізнення досліджуваних станів. Ваговий коефіцієнт -го показника визначається за формулою:

$$a_j = \frac{1 - E_j}{\sum_{i=1}^{6} (1 - E_i)}. \tag{10}$$

За такого підходу більші вагові коефіцієнти отримують показники, які сильніше розрізняють стани програм навчання в межах сформованої множини спостережень. Отримані значення a_j

використовуються на наступному етапі для побудови інтегрального показника результативності програм навчання персоналу.

Побудова інтегрального показника результативності програми навчання. Після визначення вагових коефіцієнтів показників $t_1, \dots, t_6$ результативність програми навчання може бути подана у вигляді інтегрального показника, який узагальнює значення всіх складових у межах єдиної кількісної оцінки. Оскільки всі показники мають відносний характер, належать нтервалу $[0; 1]$ та інтерпретуються в одному напрямі, тобто більше значення відповідає вищій результативності, інтегральну оцінку доцільно визначати як зважену суму показників з використанням ентропійно встановлених вагових коефіцієнтів. У загальному вигляді інтегральний показник результативності програми навчання персоналу визначається як:

$$I_T = \sum_{j=1}^{6} a_j t_j, \tag{11}$$

де a_j – ваговий коефіцієнт j-го показника, t_j – значення j-го показника, причому $\sum_{j=1}^{6} a_j = 1$, $t_j \in [0; 1]$.

За такого подання значення інтегрального показника також належить інтервалу $[0; 1]$, що забезпечує зручність його подальшої інтерпретації, порівняння між різними програмами навчання та використання в аналітичних процедурах оцінювання. Використання зваженої суми дозволяє врахувати неоднакову значущість окремих показників, яка визначається результатами ентропійного аналізу їх варіативності в межах досліджуваної множини спостережень. Отже, внесок кожного показника в інтегральну оцінку визначається його здатністю диференціювати програми навчання за рівнем результативності.

У разі застосування методики на рівні окремих підрозділів або функціонально однорідних груп персоналу для кожної організаційної одиниці d інтегральний показник може бути визначений як $I_T^{(d)} = \sum_{j=1}^{6} a_j^{(d)} t_j^{(d)}$. У такому випадку інтегральна оцінка на рівні всієї організації може бути отримана шляхом подальшого агрегування часткових оцінок підрозділів:

$$I_T^{org} = \sum_{d=1}^{m} w_d \, I_T^{(d)}, \tag{12}$$

де w_d – ваговий коефіцієнт -го підрозділу, який може визначатися за чисельністю персоналу, критичністю функцій або рівнем ризику, причому $\sum_{d=1}^{m} w_d = 1$.

Запропоноване подання інтегрального показника дозволяє використовувати його як узагальнену форму оцінювання результативності програм навчання персоналу на рівні окремої програми, підрозділу або організації в цілому. Це створює основу для порівняльного аналізу, оцінювання динаміки змін результативності та використання отриманих оцінок у процедурах підтримки управлінських рішень.

Результати сценарного моделювання свідчать про неоднорідність сформованого простору оцінювання та різну варіативність окремих показників результативності програми навчання. Як показано на рис. 1, показники поведінкової результативності та своєчасності повторного навчання зміщені в бік нижчих значень, що узгоджується з їх інтерпретацією як характеристик більш зрілих програм навчання. Водночас показник охоплення навчанням зміщений у бік вищих значень, що відображає можливість відносно широкого формального охоплення персоналу навіть за обмеженої змістової повноти програми, недостатньої актуалізації її матеріалів або невисокого поведінкового ефекту.

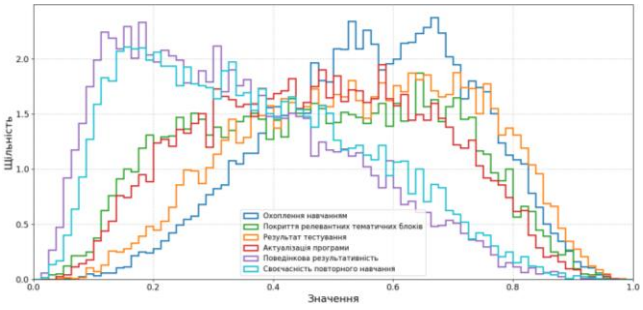

Рис. 1. Розподіли показників результативності програми навчання персоналу, отримані в результаті сценарного моделювання

Результати ентропійного аналізу показали, що найбільшу дискримінативну здатність у межах побудованої моделі мають показники поведінкової результативності та своєчасності повторного навчання. Вищі значення їх вагових коефіцієнтів свідчать, що саме ці характеристики найкраще розрізняють програми навчання за рівнем результативності. Натомість показники результату тестування та охоплення навчанням мають менший вплив на підсумкову оцінку, що вказує на їх нижчу чутливість до відмінностей між змодельованими станами програм. Графічне подання вагових коефіцієнтів наведено на рис. 2.

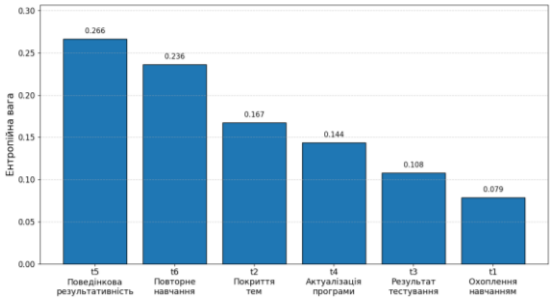

Рис. 2. Вагові коефіцієнти показників результативності програми навчання персоналу, визначені ентропійним методом

Розподіл інтегрального показника I_T, наведений на рис. 3, узагальнює вплив усіх показників з урахуванням їх вагових коефіцієнтів та відображає безперервний спектр можливих станів програм навчання персоналу. Отриманий результат підтверджує, що запропонована модель забезпечує перехід від аналізу окремих характеристик до цілісної кількісної оцінки результативності програми навчання.

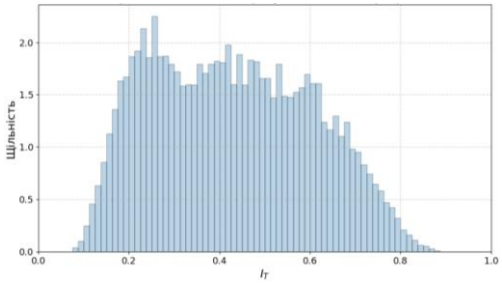

Рис. 3. Розподіл інтегрального показника результативності програми навчання персоналу I_T

Таким чином, результати сценарного моделювання підтвердили можливість формалізованого оцінювання результативності програм навчання персоналу на основі системи взаємопов'язаних показників. Використання ентропійного методу дало змогу визначити вагові коефіцієнти показників з урахуванням їх дискримінативної здатності в межах сформованого простору оцінювання. Отриманий інтегральний показник I_T забезпечує узагальнене кількісне подання результативності програми навчання та може бути використаний для порівняльного аналізу, моніторингу змін у часі й підтримки рішень щодо вдосконалення навчального процесу.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті формалізовано систему показників оцінювання результативності програм навчання персоналу з інформаційної безпеки. Запропонована система охоплює шість взаємопов'язаних показників, які відображають ключові аспекти результативності програми навчання, а саме охоплення персоналу навчанням, покриття релевантних тематичних блоків, результат підсумкового тестування, актуалізацію програми, поведінкову результативність і своєчасність повторного навчання. Для кожного показника подано формалізований спосіб визначення, що забезпечує можливість їх кількісного подання в межах єдиної моделі оцінювання.

У роботі запропоновано підхід до визначення вагових коефіцієнтів показників на основі ентропійного методу, що дало змогу встановити відносну дискримінативну здатність окремих показників у межах побудованої моделі та визначити їх внесок в інтегральну оцінку. Отримані результати показали, що найбільший внесок у диференціацію програм навчання за рівнем результативності забезпечують показники поведінкової результативності, своєчасності повторного навчання та покриття релевантних

тематичних блоків. Запропоновано інтегральний показник результативності програми навчання персоналу, який забезпечує узагальнене кількісне подання її стану та може бути використаний для порівняльного аналізу програм навчання, оцінювання динаміки їх результативності та підтримки управлінських рішень щодо вдосконалення навчального процесу.

Подальші дослідження доцільно спрямувати на уточнення системи показників для різних типів підрозділів і функціональних груп персоналу, розширення переліку поведінкових метрик, а також на адаптацію запропонованого підходу до специфіки окремих організаційних середовищ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *Information & Computer Security*, *31*(4), 463-477. https://doi.org/10.1108/ics-08-2022-0139
2. Haney, J., & Lutters, W. (2020). Security awareness training for the workforce: Moving beyond "check-the-box" compliance. *Computer*, *53*(10), 91-95. https://doi.org/10.1109/mc.2020.3001959
3. Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S., & Wasim, M. (2023). Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches. *Symmetry*, *15*(12), Article 2175. https://doi.org/10.3390/sym15122175
4. National Institute of Standards and Technology. (2024a). *Building a cybersecurity and privacy awareness and training program* (NIST Special Publication 800-50r1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-50r1
5. Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393-410. https://doi.org/10.1108/ics-07-2018-0080
6. Dahabiyeh, L. (2021). Factors affecting organizational adoption and acceptance of computer-based security awareness training tools. *Information & Computer Security*. Advance online publication. https://doi.org/10.1108/ics-12-2020-0200
7. Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity*, *8*(1), tyac006. https://doi.org/10.1093/cybsec/tyac006
8. Hijji, M., & Alam, G. (2022). Cybersecurity awareness and training (CAT) framework for remote working employees. *Sensors*, *22*(22), 8663. https://doi.org/10.3390/s22228663
9. Hillman, D., Harel, Y., & Toch, E. (2023). Evaluating organizational phishing awareness training on an enterprise scale. *Computers & Security*, *134*, 103364. https://doi.org/10.1016/j.cose.2023.103364
10. Prümmer, J., van Steen, T., & van den Berg, B. (2023). A systematic review of current cybersecurity training methods. *Computers & Security*, *134*, 103585. https://doi.org/10.1016/j.cose.2023.103585
11. Prümmer, J., van Steen, T., & van den Berg, B. (2024). Assessing the effect of cybersecurity training on end-users: A meta-analysis. *Computers & Security*, *137*, 104206. https://doi.org/10.1016/j.cose.2024.104206
12. National Institute of Standards and Technology. (2024b). *The NIST cybersecurity framework 2.0* (NIST Special Publication 1299). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.1299
13. Kő, A., Tarján, G., & Mitev, A. (2023). Information security awareness maturity: Conceptual and practical aspects in Hungarian organizations. *Information Technology & People*, *36*(8), 174-195. https://doi.org/10.1108/itp-11-2021-0849
14. Yigit Ozkan, B., van Lingen, S., & Spruit, M. (2021). The cybersecurity focus area maturity (CYSFAM) model. *Journal of Cybersecurity and Privacy*, *1*(1), 119–139. https://doi.org/10.3390/jcp1010007
15. Marshall, N., Sturman, D., & Auton, J. C. (2024). Exploring the evidence for email phishing training: A scoping review. *Computers & Security*, *139*, 103695. https://doi.org/10.1016/j.cose.2023.103695
16. Dornheim, P., & Zarnekow, R. (2023). Determining cybersecurity culture maturity and deriving verifiable improvement measures. *Information & Computer Security*. Advance online publication. https://doi.org/10.1108/ics-07-2023-0116
17. Neri, M., Benevento, E., Stefanini, A., Aloini, D., Niccolini, F., Carducci, A., Federigi, I., & Dini, G. (2024). Understanding information security awareness: Evidence from the public healthcare sector. *Information & Computer Security*. Advance online publication. https://doi.org/10.1108/ics-04-2024-0094
18. Roszkowska, E., & Wachowicz, T. (2024). Impact of normalization on entropy-based weights in Hellwig's method: A case study on evaluating sustainable development in the education area. *Entropy*, *26*(5), 365. https://doi.org/10.3390/e26050365

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Mykhailo Zaporozhchenko
Ph.D. in Cybersecurity
Associate Professor of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-0182-9497
m.zaporozhchenko@duikt.edu.ua

Svitlana Lehominova
Doctor of Sciences in Economics, Professor
Head of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-4433-5123
s.legominova@duikt.edu.ua

Dmytro Rabchun
Candidate of Technical Sciences
Associate Professor of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-5555-0910
d.rabchun@duikt.edu.ua

FORMALIZATION OF A SYSTEM OF INDICATORS FOR EVALUATING THE EFFECTIVENESS OF PERSONNEL TRAINING PROGRAMS IN INFORMATION SECURITY

Abstract. The article addresses the problem of formalizing a system of indicators for evaluating the effectiveness of personnel training programs. The relevance of the study is due to the fact that, in organizational security practice, the evaluation of such programs is often reduced to the use of separate fragmentary characteristics, including training coverage, testing results, or the frequency of training sessions, which does not provide a holistic quantitative representation of the actual effectiveness of a program. This complicates the comparison of programs, the analysis of their development dynamics, and the substantiation of managerial decisions aimed at improving the training process. The purpose of the article is to formalize a system of indicators for evaluating the effectiveness of personnel training programs by determining the composition of quantitative indicators, substantiating their formal representation, and constructing an integral evaluation. The paper proposes a system of six interrelated indicators covering the main aspects of personnel training program effectiveness, namely training coverage, coverage of relevant thematic blocks, final testing result, program updating, behavioral effectiveness, and timeliness of recurrent training. A formal expression is provided for each indicator, ensuring the possibility of its quantitative determination within a unified evaluation model. The expediency of using the entropy method to determine indicator weight coefficients is substantiated, making it possible to account for their relative discriminatory ability on a set of actual or simulated observations. To demonstrate the methodology, the paper develops a scenario-analytical model based on characteristic ranges of indicator values for training programs with different maturity levels. The scientific novelty of the study lies in the formalization of a system of indicators for evaluating the effectiveness of personnel training programs and in substantiating an approach to constructing an integral indicator based on entropy-derived weight coefficients. The obtained results showed that the greatest contribution to the differentiation of training programs by effectiveness level is made by the indicators of behavioral effectiveness, timeliness of recurrent training, and coverage of relevant thematic blocks. The practical significance of the study lies in the possibility of using the proposed model for comparative analysis of training programs, evaluation of their effectiveness dynamics, and support of decisions on improving the training process.

Keywords: cybersecurity; information security; information security management; personnel training; effectiveness evaluation; system of indicators; entropy method; modeling.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *Information & Computer Security, 31*(4), 463-477. https://doi.org/10.1108/ics-08-2022-0139
2. Haney, J., & Lutters, W. (2020). Security awareness training for the workforce: Moving beyond "check-the-box" compliance. *Computer, 53*(10), 91-95. https://doi.org/10.1109/mc.2020.3001959
3. Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S., & Wasim, M. (2023). Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches. *Symmetry, 15*(12), Article 2175. https://doi.org/10.3390/sym15122175
4. National Institute of Standards and Technology. (2024a). *Building a cybersecurity and privacy awareness and training program* (NIST Special Publication 800-50r1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-50r1
5. Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security, 27*(3), 393-410. https://doi.org/10.1108/ics-07-2018-0080
6. Dahabiyeh, L. (2021). Factors affecting organizational adoption and acceptance of computer-based security awareness training tools. *Information & Computer Security*. Advance online publication. https://doi.org/10.1108/ics-12-2020-0200
7. Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity, 8*(1), tyac006. https://doi.org/10.1093/cybsec/tyac006
8. Hijji, M., & Alam, G. (2022). Cybersecurity awareness and training (CAT) framework for remote working employees. *Sensors, 22*(22), 8663. https://doi.org/10.3390/s22228663
9. Hillman, D., Harel, Y., & Toch, E. (2023). Evaluating organizational phishing awareness training on an enterprise scale. *Computers & Security, 134*, 103364. https://doi.org/10.1016/j.cose.2023.103364
10. Prümmer, J., van Steen, T., & van den Berg, B. (2023). A systematic review of current cybersecurity training methods. *Computers & Security, 134*, 103585. https://doi.org/10.1016/j.cose.2023.103585
11. Prümmer, J., van Steen, T., & van den Berg, B. (2024). Assessing the effect of cybersecurity training on end-users: A meta-analysis. *Computers & Security, 137*, 104206. https://doi.org/10.1016/j.cose.2024.104206
12. National Institute of Standards and Technology. (2024b). *The NIST cybersecurity framework 2.0* (NIST Special Publication 1299). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.1299
13. Kő, A., Tarján, G., & Mitev, A. (2023). Information security awareness maturity: Conceptual and practical aspects in Hungarian organizations. *Information Technology & People, 36*(8), 174-195. https://doi.org/10.1108/itp-11-2021-0849
14. Yigit Ozkan, B., van Lingen, S., & Spruit, M. (2021). The cybersecurity focus area maturity (CYSFAM) model. *Journal of Cybersecurity and Privacy, 1*(1), 119–139. https://doi.org/10.3390/jcp1010007
15. Marshall, N., Sturman, D., & Auton, J. C. (2024). Exploring the evidence for email phishing training: A scoping review. *Computers & Security, 139*, 103695. https://doi.org/10.1016/j.cose.2023.103695
16. Dornheim, P., & Zarnekow, R. (2023). Determining cybersecurity culture maturity and deriving verifiable improvement measures. *Information & Computer Security*. Advance online publication. https://doi.org/10.1108/ics-07-2023-0116
17. Neri, M., Benevento, E., Stefanini, A., Aloini, D., Niccolini, F., Carducci, A., Federigi, I., & Dini, G. (2024). Understanding information security awareness: Evidence from the public healthcare sector. *Information & Computer Security*. Advance online publication. https://doi.org/10.1108/ics-04-2024-0094
18. Roszkowska, E., & Wachowicz, T. (2024). Impact of normalization on entropy-based weights in Hellwig's method: A case study on evaluating sustainable development in the education area. *Entropy, 26*(5), 365. https://doi.org/10.3390/e26050365

Отримано редакцією журналу / Received: 02.02.26
Прорецензовано / Revised: 16.02.26
Схвалено до друку / Accepted: 25.06.26

This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.