УДК 004.8:338.48:519.86
DOI https://doi.org/10.24144/2616-7700.2026.49(2).262-268

В. В. Поліщук[1], В. І. Сегляник[2]

[1] ДВНЗ «Ужгородський національний університет»,
професор кафедри програмного забезпечення систем,
доктор технічних наук, професор
volodymyr.polishchuk@uzhnu.edu.ua
ORCID: https://orcid.org/0000-0003-4586-1333

[2] ДВНЗ «Ужгородський національний університет»,
аспірант кафедри програмного забезпечення систем
vasyl.sehlianyk@uzhnu.edu.ua
ORCID: https://orcid.org/0009-0005-9958-3713

НЕЧІТКА МОДЕЛЬ ОЦІНЮВАННЯ ЦИФРОВОЇ БЕЗПЕКОВОЇ ГРАМОТНОСТІ НАСЕЛЕННЯ З УРАХУВАННЯМ СОЦІАЛЬНИХ ПРОФІЛІВ

У статті розглянуто науково-методичні аспекти розроблення нечіткої моделі оцінювання рівня цифрової безпекової грамотності населення з урахуванням соціальних профілів. Актуальність дослідження зумовлена зростанням ролі цифрової безпеки в умовах цифрової трансформації суспільства та необхідністю об'єктивного оцінювання здатності населення безпечно взаємодіяти з цифровим середовищем. Проаналізовано сучасні наукові підходи до оцінювання цифрової та кібербезпекової грамотності й обґрунтовано наукову прогалину, що полягає у відсутності комплексних моделей, які поєднують репрезентативний збір даних, формалізацію соціально-демографічних характеристик, інтегральне оцінювання та підтримку прийняття рішень.

Запропоновано нечітку модель, яка базується на формалізації кількісних і якісних демографічних характеристик населення за допомогою функцій належності та використанні вектора «цільових потреб», що формується особою, яка приймає рішення. Модель реалізує процедуру ранжування громадян за ступенем відповідності заданому соціальному профілю та дозволяє визначати кількісний показник рівня цифрової безпекової грамотності шляхом агрегування часткових оцінок. Застосування згорткового методу та системи вагових коефіцієнтів забезпечує гнучкість, відтворюваність і інтерпретованість результатів оцінювання.

Практична значущість отриманих результатів полягає у можливості використання запропонованої моделі органами державного та регіонального управління, закладами освіти, організаціями й аналітичними центрами для моніторингу рівня цифрової безпеки населення, порівняльного аналізу соціальних профілів та обґрунтування цільових заходів підвищення цифрової безпекової грамотності.

Ключові слова: цифрова безпека, соціальний профіль, нечітка модель, підтримка прийняття рішень, кібербезпека населення.

1. Вступ. Цифрова трансформація суспільства та поширення інформаційно-комунікаційних технологій посилюють значення цифрової безпеки як важливого чинника соціальної, економічної та національної безпеки. У цих умовах рівень цифрової безпекової грамотності населення визначає здатність громадян протидіяти кіберзагрозам, захищати персональні дані та безпечно користуватися цифровими сервісами, що зумовлює потребу в його об'єктивному оцінюванні.

Аналіз наукових досліджень свідчить, що більшість наявних підходів зосереджені на окремих середовищах або аспектах, але не враховують різноманіття соціально-демографічних характеристик населення та не забезпечують комплексного аналізу в розрізі соціальних профілів.

Наукова прогалина полягає у відсутності комплексних методів, що поєднують репрезентативний збір даних, формалізацію демографічних характеристик, інтегральне оцінювання та формування адресних рекомендацій для підтримки прийняття рішень.

Метою статті є розроблення та обґрунтування нечіткої моделі оцінювання рівня цифрової безпекової грамотності населення з урахуванням соціальних профілів, яка забезпечує формалізацію кількісних і якісних демографічних характеристик, інтегральне оцінювання рівня грамотності у сфері цифрової безпеки та підтримку прийняття управлінських рішень на різних територіальних рівнях.

Досягнення поставленої мети передбачає використання апарату нечіткої логіки для оброблення різнорідних даних, формування вектора «цільових потреб», ранжування громадян за відповідністю соціальним профілям і визначення кількісних показників цифрової безпекової грамотності для подальшого аналізу, моніторингу та розроблення цільових заходів.

2. Огляд літератури. Упродовж останніх років проблема оцінювання рівня цифрової та кібербезпекової грамотності активно досліджується в наукових роботах. Значна частина досліджень зосереджена на аналізі обізнаності користувачів у межах окремих середовищ, насамперед організаційного та освітнього. У роботах [1–2] розглянуто підходи до підвищення та вимірювання інформаційної безпекової обізнаності працівників, а також чинники формування політик кібербезпеки на рівні окремих країн. Водночас такі дослідження орієнтовані переважно на інституційний рівень і не враховують різноманіття соціально-демографічних профілів населення.

Окремий напрям досліджень стосується розроблення та валідації шкал і індикаторів оцінювання цифрової або кібербезпекової грамотності. У роботах [3–4] показано, що наявні підходи істотно різняться за структурою, набором показників і способами інтерпретації результатів, що ускладнює їх порівняння та повторне використання. Водночас такі дослідження здебільшого орієнтовані на окремі групи користувачів і не формують універсальної інтегральної процедури оцінювання для різних соціальних профілів.

Значний масив праць присвячено ефективності освітніх і тренінгових заходів у сфері кібербезпеки [5–6]. Хоча їх результати підтверджують позитивний вплив окремих втручань, ці підходи переважно зосереджені на ізольованих аспектах і не забезпечують комплексного оцінювання рівня цифрової безпекової грамотності населення [7–8].

Окрему групу становлять дослідження поведінкових і психологічних моделей кібербезпекової поведінки [9–10]. Такі роботи поглиблюють розуміння мотиваційних чинників і ризиків, однак не інтегруються з процедурами агрегування демографічних характеристик і не орієнтовані на підтримку управлінських рішень у розрізі соціальних профілів.

Отже, сучасні підходи до оцінювання цифрової та кібербезпекової грамотності залишаються фрагментарними. У науковій літературі бракує комплексних моделей, що поєднують збір даних, формалізацію демографічних характеристик, інтегральне оцінювання та формування адресних рекомендацій, що й зумовлює актуальність запропонованого нечіткого підходу.

3. Матеріали та методи. Дослідження проводиться на певній терито-

рії R, яка може представляти місто, регіон або країну. Населення цієї території позначається як $C = \{c_1; c_2; \ldots; c_n\}$. По громадянах враховуються різні демографічні характеристики, що утворюють деякий соціальний профіль $SP = \{sp_1; sp_2; \ldots; sp_k\}$. Потрібно здійснити оцінювання рівня грамотності населення у сфері цифрової безпеки деякої території у розрізі різних соціальних профілів.

Для отримання вхідних даних здійснюється опитування респондентів. Збір вхідної інформації відбувається за допомогою текстової анкети, розробленої на основі системи критеріїв K, які об'єднані по групах G. Використовуючи раніше розроблений згортковий метод відбувається визначення агрегованого рівня обізнаності громадян у сфері кібербезпеки ($\vartheta(c)$) та загального рівня в межах досліджуваної території – M_S [11]. Після цього, отримані дані йдуть на обчислення за допомогою нечіткої моделі оцінювання рівня грамотності населення різних соціальних профілів у сфері цифрової безпеки — M_{DS}.

Нечітка модель може бути представлена у вигляді оператора:

$$M_{DS}(R,\ C, SP,\ \vartheta\,(c))|\, Y(f). \tag{1}$$

Оператор M_{DS} на основі вхідних даних R, C, SP, $\vartheta(c)$ ставить у відповідність вихідне значення $Y(f)$ — кількісний рівень грамотності населення у сфері цифрової безпеки деякого соціального профілю (sp).

Нехай громадянин C описується множиною демографічних характеристик $S = \{s_1, s_2, \ldots, s_m\}$, які формують відповідний соціальний профіль $SP = \{sp_1, sp_2, \ldots, sp_k\}$. Оскільки ці характеристики мають як кількісну, так і якісну природу, для забезпечення їх коректного порівняння та подальшої обробки вони формалізуються та нормуються за єдиною шкалою.

У межах дослідження соціальний профіль громадянина формується на основі сукупності демографічних характеристик, зокрема статі, віку, соціально-економічного статусу, рівня освіти, доходу та сімейного стану. Оскільки ці характеристики мають кількісну й якісну природу, для їх узгодженого аналізу застосовуються функції належності, що дають змогу формалізувати вихідні значення та привести їх до єдиної нормованої шкали. У загальному вигляді для кожної демографічної характеристики d_u вводиться функція належності $\mu_{d_u}(x) : X_u \to [0; 1]$, яка ставить у відповідність значенню ознаки x ступінь його належності до заданого терму або цільового стану. Для кількісних демографічних характеристик, зокрема віку та доходу, використовуються лінійні або трапецієподібні функції належності на шкалі $[0; 1]$. Для якісних характеристик, таких як рівень освіти, сімейний стан чи соціально-економічний статус, застосовується дискретне кодування з подальшим заданням відповідних функцій належності до лінгвістичних термів. Такий підхід забезпечує уніфіковане подання різнорідних демографічних ознак у числовій формі та створює основу для подальшого застосування апарату нечіткої логіки.

Дане дослідження спрямоване на визначення рівня грамотності населення у сфері цифрової безпеки у розрізі різних соціальних профілів $SP = \{sp_1; sp_2; \ldots; sp_k\}$. Соціальний профіль утворюється групуванням різних демографічних характеристик S шляхом задання деякого правила ОПР — τ.

У дослідженні формування соціального профілю $SP(\tau)$ відповідно до правил особи, що приймає рішення (τ), інтерпретується як задання «цільової потре-

би». Відповідно, вектор цільових потреб визначається як сукупність демографічних характеристик умовної групи громадян, для якої оцінюється рівень цифрової безпекової грамотності з метою подальшого аналізу та підтримки прийняття рішень.

Нехай отримані нормовані дані щодо громадян C, сформовані відповідно до їх демографічних характеристик у досліджуваному регіоні R, подаються у вигляді матриці рішень:

$$SPC = \begin{pmatrix} sp_1(c_1) & sp_1(c_2) & \dots & sp_1(c_n) \\ sp_2(c_1) & sp_2(c_2) & \dots & sp_2(c_n) \\ \dots & \dots & \dots & \dots \\ sp_k(c_1) & sp_k(c_2) & \dots & sp_k(c_n) \end{pmatrix} \tag{2}$$

На наступному етапі особа, що приймає рішення, задає k-вимірний вектор цільових потреб для оцінювання рівня цифрової безпекової грамотності відповідного соціального профілю. Цей вектор використовується для формалізованого опису вимог до заданого профілю та надалі позначається як $Z(\tau) = Z^* = (\widehat{sp}_1, \widehat{sp}_2, \dots, \widehat{sp}_k)$.

Далі формується ранжувальний ряд громадян $C = \{c_1, c_2, \dots, c_n\}$, у якому перші позиції займають альтернативи, що найбільшою мірою відповідають заданому вектору «цільових потреб» соціального профілю. Запропонований підхід ґрунтується на пошуку рішень, які за сукупністю демографічних характеристик є максимально наближеними до визначеного вектора.

Для цього використовується матриця SPC разом із вектором $Z(\tau)$, на основі яких визначається система показників, що характеризують ступінь близькості елементів матриці SPC до відповідних компонентів вектора «цільових потреб» заданого соціального профілю:

$$q_{ui} = 1 - \frac{|\overline{sp_u} - sp_u(c_i)|}{\max\left\{\overline{sp_u} - \min\limits_i (sp_u(c_i)) ; \max\limits_i (sp_u(c_i)) - \overline{sp_u}\right\}}, \quad u = \overline{1,k};\ \ i = \overline{1,n}. \tag{3}$$

Сформована матриця $Q = \{q_{ui}\}$ відображає ступінь близькості громадян c_iдо вектора цільових потреб Z^* за кожною демографічною характеристикою. При цьому особа, що приймає рішення, може формувати Z^* не за всіма показниками, а лише за їх вибраною множиною, що відповідно зменшує розмірність матриці рішень SPC.

На наступному етапі особа, що приймає рішення, задає вагові коефіцієнти $\{v_1, v_2, \dots, v_k\}$ для кожної демографічної характеристики соціального профілю SP, наприклад, у межах інтервалу $[1; 10]$. З метою забезпечення порівнюваності показників здійснюється нормування вагових коефіцієнтів:

$$w_u = \frac{v_u}{\sum\limits_{u=1}^{k} v_u}, \quad u = \overline{1,k}; \quad w_u \in [0;1]\,. \tag{4}$$

Вагові коефіцієнти v_u доцільно визначати на основі експертної процедури, зокрема шляхом попарного порівняння важливості демографічних характеристик або за бальною шкалою з подальшим нормуванням за умовою $\sum\limits_{u=1}^{m} v_u = 1$.

Це підвищує обґрунтованість, відтворюваність і зменшує суб'єктивність оцінювання.

На завершальному етапі здійснюється формування ранжувального ряду громадян $C = \{c_1, c_2, \ldots, c_n\}$ відносно «цільових потреб» заданого соціального профілю. Не обмежуючи загальності підходу, для агрегування часткових оцінок застосовується згортковий метод, зокрема середня згортка, яка має такий вигляд:

$$\rho(c_i) = \sum_{u=1}^{k} w_u \cdot q_{ui}. \tag{5}$$

На наступному етапі визначається кількісний рівень цифрової безпекової грамотності заданого соціального профілю. Для цього особа, що приймає рішення, задає кількість громадян r, після чого з ранжувального ряду $A = (A_1, A_2, \ldots, A_n)$ відбираються перші r альтернатив. Для цієї підмножини на основі агрегованого рівня обізнаності $\vartheta(c)$ обчислюється середнє значення, яке інтерпретується як кількісна оцінка рівня цифрової безпекової грамотності відповідного соціального профілю:

$$Y(f) = \frac{1}{r} \sum_{d=1}^{r} \vartheta(c_d). \tag{6}$$

Коли $m_{dsp}(sp) \to 1$ тоді буде високий рівень грамотності населення у сфері цифрової безпеки вибраного соціального профілю.

У результаті було відібрано сукупність громадян, демографічні характеристики яких є найбільш наближеними до заданого особою, що приймає рішення, соціального профілю. На основі отриманої вибірки надалі обчислено середній рівень грамотності у сфері цифрової безпеки.

4. Висновки та перспективи подальших досліджень. У ході дослідження розроблено нечітку модель оцінювання рівня цифрової безпекової грамотності населення з урахуванням соціальних профілів. Запропонований підхід забезпечує комплексне оцінювання на основі репрезентативних емпіричних даних, отриманих шляхом анкетування. Модель ґрунтується на формалізації кількісних і якісних демографічних характеристик за допомогою функцій належності, що забезпечує їх узгоджене порівняння та інтегральне оцінювання.

Запровадження вектора «цільових потреб», сформованого особою, що приймає рішення, дає змогу ранжувати громадян за ступенем відповідності заданому соціальному профілю. Використання матриці відносних оцінок, нормованих вагових коефіцієнтів і згорткового методу забезпечує прозору, відтворювану та інтерпретовану процедуру оцінювання. На цій основі визначається підмножина громадян, найбільш наближених до обраного профілю, та обчислюється кількісний показник рівня цифрової безпекової грамотності.

Практична значущість моделі полягає у можливості її застосування для моніторингу стану цифрової безпеки населення, порівняльного аналізу соціальних профілів і формування адресних управлінських рішень щодо підвищення цифрової грамотності.

Перспективи подальших досліджень пов'язані з апробацією запропонованої моделі на реальних вибірках респондентів, поданням модельних числових при-

кладів її застосування для різних соціальних профілів та розширенням емпіричної бази на різні територіальні рівні.

Конфлікт інтересів

Поліщук Володимир Володимирович, член редакційної колегії, є автором цієї статті та не брав участі в редакційному розгляді й ухваленні рішення щодо рукопису. Опрацювання рукопису здійснювалося незалежним редактором. Інші редактори заявляють про відсутність конфлікту інтересів.

Фінансування

Це дослідження виконано в межах наукових проєктів молодих учених «Захист інформаційної безпеки при управлінні проєктами міжнародного співробітництва на засадах гарантування національної безпеки України» (DB-921M) та «Захист персональних даних в умовах розвитку штучного інтелекту та Інтернету речей: правові й технічні аспекти» (DB-924M), що фінансуються Міністерством освіти і науки України.

Доступність даних

Усі дані доступні в цифровій або графічній формі в основному тексті рукопису.

Використання штучного інтелекту

Автори підтверджують, що при створенні даної роботи вони не використовували технології штучного інтелекту.

Внесок авторів

В. В. Поліщук: концептуалізація, формальний аналіз, методологія, написання — оригінальний проект, написання — рецензування та редагування. В. І. Сегляник: курація даних, формальний аналіз, методологія, написання — оригінальний проект, написання — рецензування та редагування.

Авторські права © (2026). Поліщук В. В., Сегляник В. І. Ця робота ліцензується відповідно до Creative Commons Attribution 4.0 International License.

Список використаної літератури

1. Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees' information security awareness in private and public organisations: A systematic literature review. *Computers & Security,* 106, Article 102267. https://doi.org/10.1016/j.cose.2021.102267
2. Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security,* 120, Article 102820. https://doi.org/10.1016/j.cose.2022.102820
3. Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon,* 9(3), Article e14234. https://doi.org/10.1016/j.heliyon.2023.e14234

4. Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences,* 14(6), Article 588. https://doi.org/10.3390/educsci14060588
5. Argyridou, E., Nifakos, S., Laoudias, C., & et al. (2023). Cyber hygiene methodology for raising cybersecurity and data privacy awareness in health care organizations: Concept study. *Journal of Medical Internet Research,* 25, Article 41294. https://doi.org/10.2196/41294
6. Hull, D. M., Schuetz, S. W., & Lowry, P. B. (2023). Tell me a story: The effects that narratives exert on meaningful-engagement outcomes in antiphishing training. *Computers & Security,* 129, Article 103252. https://doi.org/10.1016/j.cose.2023.103252
7. Berens, B. M., Mossano, M., & Volkamer, M. (2024). Taking 5 minutes protects you for 5 months: Evaluating an anti-phishing awareness video. *Computers & Security,* 137, Article 103620. https://doi.org/10.1016/j.cose.2023.103620
8. Kävrestad, J., Hagberg, A., Nohlberg, M., Rambusch, J., & et al. (2024). Design principles for cognitively accessible cybersecurity training. *Computers & Security,* 137, Article 103630. https://doi.org/10.1016/j.cose.2023.103630
9. Kiran, U., Khan, N., Murtaza, H., & Farooq, A. (2025). Explanatory and predictive modeling of cybersecurity behaviors using Protection Motivation Theory. *Computers & Security,* 149, Article 104204. https://doi.org/10.1016/j.cose.2024.104204
10. Prümmer, J., van Steen, T., & van den Berg, B. (2025). Assessing the effect of cybersecurity training on end-users: A meta-analysis. *Computers & Security. Advance online publication.* Article 104206. https://doi.org/10.1016/j.cose.2024.104206
11. Polishchuk, I., Petrushko, I., Sehlianyk, V., & Matei, A. (2025). Intellectual model for assessing the level of citizens' awareness in the field of cybersecurity. *Herald of Khmelnytskyi National University. Technical Sciences,* 357(5.1), 367–374. https://doi.org/10.31891/2307-5732-2025-357-47

Polishchuk V., Sehlianyk V. A fuzzy model for assessing digital cybersecurity literacy of the population considering social profiles.

The article addresses the scientific and methodological aspects of developing a fuzzy model for assessing the level of digital (cybersecurity) literacy of the population about social profiles. The relevance of the study is driven by the growing importance of digital security in the context of digital transformation and the need for an objective assessment of the population's ability to safely interact with the digital environment. Contemporary scientific approaches to evaluating digital and cybersecurity literacy are analyzed, and a research gap is identified, which lies in the absence of comprehensive models that integrate representative data collection, formalization of socio-demographic characteristics, integral assessment, and decision support.

A fuzzy model is proposed that is based on the formalization of quantitative and qualitative demographic characteristics using membership functions and the application of a "target needs" vector defined by the decision-maker. The model implements a procedure for ranking individuals according to their degree of conformity with a specified social profile and enables the determination of a quantitative indicator of digital cybersecurity literacy through the aggregation of partial assessments. The use of a convolution-based aggregation method and a system of weight coefficients ensure flexibility, reproducibility, and interpretability of the assessment results.

The practical significance of the obtained results lies in the applicability of the proposed model by state and regional authorities, educational institutions, organizations, and analytical centers for monitoring the level of digital security literacy of the population, conducting comparative analyses of social profiles, and substantiating targeted measures aimed at improving digital cybersecurity literacy.

Keywords: digital security, social profile, fuzzy model, decision support, population cybersecurity literacy.

Отримано: 17.03.2026 Прийнято: 03.04.2026 Опубліковано: 30.04.2026