https://doi.org/10.31891/2307-5732-2025-357-47
УДК 519.86

ПОЛІЩУК ІННА
ДВНЗ «Ужгородський національний університет»
Кошицький технічний університет
https://orcid.org/0009-0002-6395-4744
e-mail: inna.polishchuk@uzhnu.edu.ua
ПЕТРУШКО ІРИНА
ДВНЗ «Ужгородський національний університет»
https://orcid.org/0009-0008-2303-7427
e-mail: irina.petrushko@uzhnu.edu.ua
СЕГЛЯНИК ВАСИЛЬ
ДВНЗ «Ужгородський національний університет»
https://orcid.org/0009-0005-9958-3713
e-mail: vasyl.sehlianyk@uzhnu.edu.ua
МАТЕЙ АНДРІЙ
ДВНЗ «Ужгородський національний університет»
https://orcid.org/0009-0001-0280-1763
e-mail: andrej.matey@uzhnu.edu.ua

ІНТЕЛЕКТУАЛЬНА МОДЕЛЬ ОЦІНЮВАННЯ РІВНЯ ОБІЗНАНОСТІ ГРОМАДЯН У СФЕРІ КІБЕРБЕЗПЕКИ

У роботі запропоновано інтелектуальну модель оцінювання рівня обізнаності громадян у сфері кібербезпеки. Вона реалізується як формалізований підхід до обробки даних анкетування з урахуванням багатьох чинників, які впливають на безпечну цифрову поведінку. Розроблена модель поєднує методи нечітких множин, фазифікації даних та інтелектуального аналізу знань. Це забезпечує якісний аналіз знань користувачів щодо захисту персональних даних, цифрової гігієни, виявлення загроз та відповідей на кіберінциденти. Методика дозволяє проводити оцінювання на рівні окремих громадян або територій різного масштабу: міста, регіону чи держави. На основі отриманих результатів здійснюється лінгвістична класифікація рівня обізнаності. Апробація моделі проведена на прикладі Закарпатської області на основі опитування 315 респондентів у 2025 році. Результати дають змогу виявити прогалини в знаннях, сформувати інформаційні кампанії, адаптувати освітні програми та зміцнити інформаційну безпеку.

Ключові слова: *кібербезпека; цифрова грамотність; підтримка прийняття рішень; експертне оцінювання; нечіткі множини; інформаційна безпека.*

POLISHCHUK INNA
Uzhhorod National University
Technical University of Kosice
PETRUSHKO IRYNA
SEHLIANYK VASYL
MATEI ANDRII
Uzhhorod National University

INTELLECTUAL MODEL FOR ASSESSING THE LEVEL OF CITIZENS' AWARENESS IN THE FIELD OF CYBERSECURITY

This study presents an intelligent model for assessing the level of public awareness in the field of cybersecurity. The proposed model serves as a formalized approach that analyzes survey data, considering a broad range of factors that influence safe digital behavior. It integrates fuzzy sets, data fuzzification techniques, and elements of computational intelligence to ensure a comprehensive and flexible evaluation. The model enables a qualitative analysis of citizens' knowledge regarding personal data protection, digital hygiene practices, online threat identification, and appropriate responses to cybersecurity incidents. Importantly, this approach accounts for the subjectivity and vagueness of human judgments, which are common in social research where objective measurements are often limited. A key advantage of the approach is its scalability, enabling the assessment of awareness both at the level of individual citizens and across broader populations – be it a city, region, or entire country. Based on the processed data, the model produces a linguistic classification of awareness levels, supporting the identification of critical knowledge gaps in specific groups. These insights are essential for guiding public education strategies, designing targeted information campaigns, and enhancing national cybersecurity policies. The model was tested and validated using empirical data collected in Zakarpattia Oblast (Ukraine) in 2025. A total of 315 respondents participated in the survey. The findings demonstrate the model's effectiveness in identifying trends and vulnerabilities in digital behavior. By offering actionable insights, the model contributes to strengthening digital literacy and improving cybersecurity resilience at various socio-demographic levels. Further application of this model may support the development of regional cyber hygiene standards and help optimize educational efforts aimed at different target groups.

Keywords: *cybersecurity; digital literacy; decision support; expert assessment; fuzzy sets; information security.*

Стаття надійшла до редакції / Received 30.07.2025
Прийнята до друку / Accepted 25.08.2025

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

У сучасному цифровому суспільстві питання кібербезпеки набуває особливої актуальності, оскільки стрімке поширення інформаційно-комунікаційних технологій супроводжується зростанням

кіберзагроз, що впливають як на окремих громадян, так і на державні інституції. Обізнаність населення щодо основ безпечної поведінки в цифровому середовищі є ключовим чинником формування національної стійкості до інформаційних атак, витоків персональних даних та інших форм цифрового ризику.

Низький рівень кіберграмотності населення, особливо у регіонах, обмежує ефективність реалізації державних політик у сфері інформаційної безпеки, стримує розвиток цифрової економіки та підвищує вразливість суспільства до кіберінцидентів. Постає необхідність у створенні ефективних моделей оцінювання рівня обізнаності громадян у сфері кібербезпеки, які б дозволяли не лише проводити моніторинг поточної ситуації, а й формувати підґрунтя для цілеспрямованих інформаційно-просвітницьких заходів.

Розв'язання цієї проблеми тісно пов'язане з актуальними завданнями у сфері соціальної кібербезпеки, цифрової освіти, управління інформаційними ризиками та впровадження інтелектуальних систем підтримки прийняття рішень. З наукової точки зору дослідження спрямоване на розвиток методів інтелектуального аналізу знань, фазифікації та агрегування експертної інформації. З практичного боку – надання інструментів для оцінки кіберобізнаності, які можуть бути використані державними структурами, освітніми закладами, громадськими організаціями та іншими зацікавленими сторонами для підвищення цифрової безпеки населення.

Аналіз досліджень та публікацій

Проблематика кібербезпеки на сучасному етапі активно розробляється вітчизняними та зарубіжними науковцями, що зумовлено глобалізацією інформаційного простору та зростанням загроз цифрового характеру. У працях [1-2], розглядаються фундаментальні аспекти безпеки інформаційних систем, поведінкові чинники користувачів, а також моделі ризиків, пов'язаних із цифровими загрозами [3-4]. Значна увага приділяється також формуванню культури кібербезпеки серед населення [5] та розробці освітніх програм для підвищення обізнаності [6].

На українському науковому просторі вивчення питань цифрової безпеки здійснюється переважно у контексті державної політики, правового регулювання, а також окремих аспектів цифрової грамотності [7]. Вітчизняні дослідники, зокрема, акцентують увагу на необхідності інтеграції питань кібергігієни в систему освіти, формуванні базових навичок безпечної поведінки в мережі серед широких верств населення, зокрема молоді та осіб працездатного віку [7-8]. Проте у більшості досліджень відсутні формалізовані підходи до оцінювання рівня такої обізнаності.

Сучасні методи оцінювання знань у сфері кібербезпеки здебільшого базуються на опитуваннях, які мають переважно описовий характер [9]. У той же час зростає інтерес до застосування інтелектуальних моделей і методів нечіткого аналізу, які дозволяють глибше аналізувати поведінкові та когнітивні аспекти користувачів [10]. Дослідження, у яких застосовуються фазифікація, нечіткі множини та агрегування показників, демонструють високу ефективність у соціотехнічному аналізі, однак залишаються недостатньо представленими в контексті оцінювання кіберобізнаності.

Таким чином, наявний стан досліджень свідчить про актуальність подальшої розробки інтелектуальних моделей, що поєднують методи анкетного збору даних, стандартизації показників, фазифікації та агрегування результатів. Це дозволить створити ефективний інструментарій для оцінювання рівня обізнаності громадян у сфері кібербезпеки з можливістю практичного застосування для формування політик цифрової безпеки.

Формулювання цілей статті

Основною метою наукового дослідження є розроблення інтелектуальної моделі оцінювання рівня обізнаності громадян у сфері кібербезпеки, яка дозволить не лише здійснювати кількісну та якісну оцінку поточного стану, але й формувати обґрунтовані рекомендації для підвищення рівня цифрової грамотності населення.

Виклад основного матеріалу

Дослідження проводиться на певній території R, яка може представляти місто, регіон або країну. Населення цієї території позначається як $\mathrm{C} = \{\mathrm{c}_1; \mathrm{c}_2; \ldots; \mathrm{c}_\mathrm{n}\}$. Метою є оцінити рівень обізнаності громадян у сфері кібербезпеки. Для отримання необхідних даних заплановано проведення опитування респондентів. Збір вхідної інформації здійснюється за допомогою текстової анкети, розробленої на основі системи критеріїв K, які об'єднані по групах G. Анкета-питальник по критеріях оцінювання разом із системою опрацювання даних об'єднані в інформаційну модель оцінювання рівня обізнаності громадян у сфері кібербезпеки – $\mathrm{K_S}$. Фазифіковані вхідні дані за інформаційною моделлю обчислюються за згортковим методом визначення агрегованого рівня обізнаності громадян у сфері кібербезпеки та загального рівня в межах досліджуваної території – $\mathrm{M_S}$.

Формальна постановка інтелектуальної моделі оцінювання рівня обізнаності громадян у сфері кібербезпеки може бути представлена у вигляді оператора:

$$\Sigma(R, C, K_S, M_S) \to Y. \quad (1)$$

Оператор Σ на основі вхідних даних $\mathrm{R, C, K_S, M_S}$ ставить у відповідність вихідне значення Y. Вихідне значення Y складається з наступних величин: $\vartheta(C)$ – агрегований рівень обізнаності громадянина у сфері кібербезпеки; ϑ_R – загальний рівень обізнаності громадян у сфері кібербезпеки

для досліджуваної територіїR;LFC – лінгвістичний рівень обізнаності громадян у сфері кібербезпеки для досліджуваної території.

Для наочного представлення дослідження наведена структурна схема інтелектуальної моделі оцінювання рівня обізнаності громадян у сфері кібербезпеки (рис. 1).

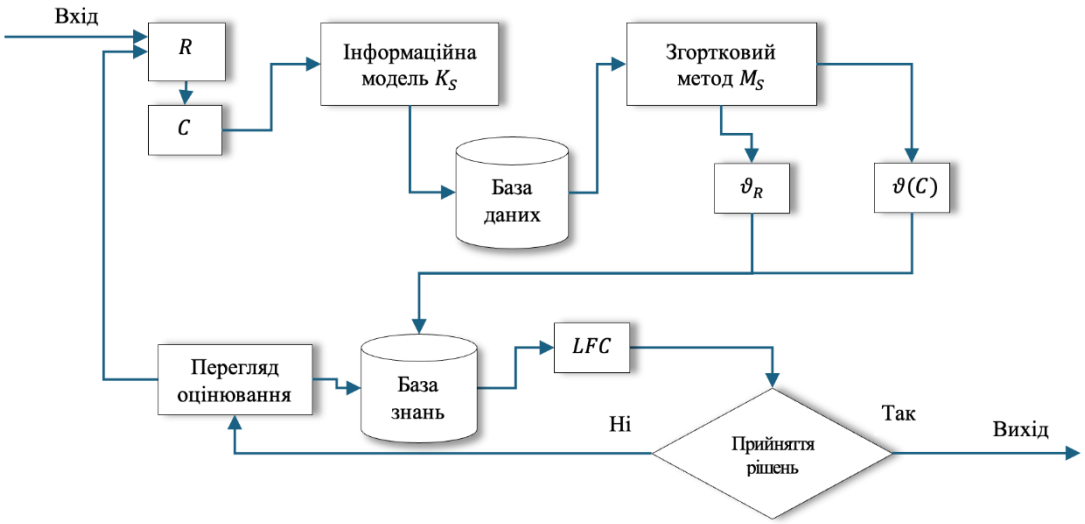

Рис. 1. Структурна схема інтелектуальної моделі

Рис. 1. відображає структурну схему інтелектуальної моделі оцінювання рівня обізнаності громадян у сфері кібербезпеки. Опрацювання вхідних даних відбувається за інформаційною моделлю оцінювання – K_S. Тут на вхід подаються зібрані вхідні дані від громадян Cна досліджуваній території R. Після їх опрацювання отримуються нормовані оцінки, що формують базу даних дослідження. Далі дані опрацьовуються згортковим методом (M_S). Тут визначається агрегований рівень обізнаності громадянина у сфері кібербезпеки $\vartheta(C)$ та загальний рівень обізнаності громадян у сфері кібербезпеки для досліджуваної території (ϑ_R). Отримані оцінки формують базу знань дослідження та на їх основі виводиться лінгвістичний рівень обізнаності громадян у сфері кібербезпеки для досліджуваної території (LFC). Особа, що приймає рішення (ОПР) аналізує отримані вихідні знання та приймає подальші рішення. В протилежному випадку відбувається перегляд оцінювання.

Інформаційна модель оцінювання рівня обізнаності громадян у сфері кібербезпеки

На першому етапі потрібно отримати вхідні дані використовуючи інформаційну модель оцінювання. Для цього пропонується відкрита множина критеріїв, що уможливлює дослідити різні аспекти обізнаності громадян у сфері кібербезпеки. Критерії оцінювання розбиті на чотири групи. Респондентам слід оцінити свої знання за бальною шкалою від 1 до 10, де 1 балів означає «абсолютно незначний» рівень знань, а 10 балів – «абсолютно значущий» рівень. Проміжні бали відображають середнє значення.

G_1– основи кібербезпеки. Дана група охоплює критерії, спрямовані на оцінювання базових знань користувачів щодо захисту особистих даних, фішингу, шкідливого програмного забезпечення, управління паролями та застосування двофакторної автентифікації.

K_{11}– Як ви оцінюєте свої знання щодо загроз для особистих даних в Інтернеті?

K_{12}– Наскільки добре ви розумієте, що таке фішинг?

K_{13}– Як ви оцінюєте свої знання про шкідливе програмне забезпечення (малваре)?

K_{14}– Як часто ви змінюєте свої паролі?

K_{15}– Наскільки добре ви використовуєте для паролів комбінації великих і малих літер, цифр і спеціальних символів?

K_{16}– Як ви оцінюєте свої знання щодо методів зберігання паролів (на папері, в браузері, використання менеджера паролів)?

K_{17} – Оцініть свої знання щодо використання двофакторної автентифікації для захисту акаунтів.

G_2– захист особистих даних в Інтернеті. Група охоплює критерії, що стосуються обізнаності користувачів щодо способів захисту персональної інформації, безпечного використання вебресурсів, налаштувань конфіденційності в соціальних мережах та реагування на загрози, пов'язані з компрометацією акаунтів.

K_{21}– Як ви оцінюєте свої знання про особисті дані та їх захист?

K_{22}– Як ви оцінюєте свої знання щодо методів захисту особистих даних в Інтернеті?

K_{23}– Наскільки уважно ви ставитесь до безпеки при наданні персональних даних на сайтах без захищеного з'єднання (https)?

K_{24}– Як ви оцінюєте свої знання щодо налаштувань конфіденційності в соціальних мережах?

K_{25}– Наскільки часто ви перевіряєте, хто має доступ до ваших особистих даних у соціальних мережах?

K_{26}– Як ви оцінюєте свої знання щодо реагування на повідомлення про скомпрометований акаунт?

G_3– виявлення кіберзагроз. Дана група охоплює критерії, спрямовані на оцінювання знань користувачів щодо розпізнавання небезпечних вебресурсів, виявлення шкідливого програмного забезпечення, реагування на підозрілі електронні листи та розуміння основних типів кіберзагроз, зокрема DDoS-атак.

K_{31}– Як ви оцінюєте свої знання щодо визначення безпеки вебсайту для відвідування?

K_{32}– Наскільки часто ви оновлюєте антивірусне програмне забезпечення на своїх пристроях?

K_{33}– Як ви оцінюєте свої знання щодо дій при отриманні електронного листа від невідомого відправника з підозрілим вкладенням?

K_{34}– Наскільки ви обізнані щодо поняття DDoS-атаки?

K_{35}– Як ви оцінюєте свої знання щодо виявлення шкідливого програмного забезпечення на пристроях?

G_4 – підвищення обізнаності та реагування на інциденти. Група охоплює критерії, що визначають рівень участі користувачів у навчаннях з кібербезпеки, їхню поінформованість щодо дій у разі кіберінцидентів та використання додаткових засобів захисту, таких як VPN, антивіруси та фаєрволи.

K_{41}– Як часто ви берете участь у навчаннях або тренінгах з кібербезпеки?

K_{42}– Наскільки ви обізнані, до кого звертатися в разі виявлення кіберзагрози?

K_{43}– Як би ви оцінили свої знання щодо реагування на повідомлення про кібератаку на вашу організацію чи компанію?

K_{44}– Як ви оцінюєте свої знання щодо використання додаткових програм для захисту від кіберзагроз (VPN, антивіруси, фаєрволи)?

Після опитування громадян, отримуються вхідні дані, що представляють собою бальні оцінки по критеріях K_{fp}. Такі оцінки позначаються e_{fp} де f – номер групи ($f = \overline{1,4}$), p – номер критерію у відповідній групі ($p = \overline{1,l}$).

Для можливості порівняння даних потрібно перейти від кількісних бальних оцінок до нормованих. Тому спочатку, в межах груп критеріїв потрібно отримати одну загальну оцінку:

$$\delta_f(c_i) = \sum_{p=1}^{l} e_{fp}(c_i), f = \overline{1,4}, i = \overline{1,n}. \quad (2)$$

Де i – номер респондента.

Використовуючи інтелектуальний аналіз знань та одновимірні функції належності пропонується здійснити фазифікацію вхідних даних. При цьому, оскільки чим більша сума балів, тим вища обізнаність громадян. Тому тут пропонується використовувати S-подібні функції належності. Оскільки кожна з груп критеріїв має різну кількість критеріїв, тому потрібно побудувати функції належності для кожної групи критеріїв. Наприклад, пропонується використати квадратичний S-сплайн. Параметри функції належності задаються, як мінімальна та максимальна можлива набрана оцінка в групі критеріїв. Тоді для запропонованих груп критеріїв G_1, G_2, G_3, G_4 функції належності будуть наступні:

$$\mu_1(c_i) = \begin{cases} 0, & \delta_1(c_i) \le 7; \\ \frac{(\delta_1(c_i)-7)^2}{1922}, & 7 < \delta_1(c_i) \le 38; \\ 1 - \frac{(69-\delta_1(c_i))^2}{1922}, & 38 < \delta_1(c_i) < 69; \\ 1, & \delta_1(c_i) \ge 69. \end{cases} \quad (3)$$

$$\mu_2(c_i) = \begin{cases} 0, & \delta_2(c_i) \le 6; \\ \frac{(\delta_2(c_i)-6)^2}{1458}, & 6 < \delta_2(c_i) \le 33; \\ 1 - \frac{(60-\delta_2(c_i))^2}{1458}, & 33 < \delta_2(c_i) < 60; \\ 1, & \delta_2(c_i) \ge 60. \end{cases} \quad (4)$$

$$\mu_3(c_i) = \begin{cases} 0, & \delta_3(c_i) \le 5; \\ \frac{(\delta_3(c_i)-5)^2}{968}, & 5 < \delta_3(c_i) \le 27; \\ 1 - \frac{(49-\delta_3(c_i))^2}{968}, & 27 < \delta_3(c_i) < 49; \\ 1, & \delta_3(c_i) \ge 49. \end{cases} \quad (5)$$

$$\mu_4(c_i) = \begin{cases} 0, & \delta_4(c_i) \le 4; \\ \dfrac{(\delta_4(c_i) - 4)^2}{648}, & 4 < \delta_4(c_i) \le 22; \\ 1 - \dfrac{(40 - \delta_4(c_i))^2}{648}, & 22 < \delta_4(c_i) < 40; \\ 1, & \delta_4(c_i) \ge 40. \end{cases} \quad (6)$$

Де $\delta_1(c_i)$, $\delta_2(c_i)$, $\delta_3(c_i)$, $\delta_4(c_i)$ – отримана кількість балів по групах критеріїв, i–м громадянином, $i = \overline{1,n}$. Отримані оцінки $\mu_1(c_i)$, $\mu_2(c_i)$, $\mu_3(c_i)$, $\mu_4(c_i)$ нормовані та характеризують рівень обізнаності громадян у сфері кібербезпеки по відповідній групі критеріїв оцінювання.

Далі представляється, згортковий метод визначення агрегованого рівня обізнаності громадян у сфері кібербезпеки та загального рівня в межах досліджуваної території. Основна ідея – це врахування важливості груп критеріїв, що представляють собою різні аспекти оцінювання обізнаності громадян у сфері кібербезпеки. Для цього пропонується ОПР задати вагові коефіцієнти для кожної групи критеріїв G_f, наприклад з інтервалу [1; 10]: v_1, v_2, v_3, v_4. Далі відбувається нормування вагових коефіцієнтів:

$$w_f = \frac{v_f}{\sum_{f=1}^{4} v_f}, w_f \in [0; 1]. \quad (7)$$

Використовуючи згортковий підхід відбувається перехід до агрегованого рівня обізнаності громадянина у сфері кібербезпеки. Наприклад, середня згортка буде мати вигляд:

$$\vartheta(c_i) = \sum_{f=1}^{4} w_f \cdot \mu_f(c_i), i = \overline{1,n}. \quad (8)$$

Отже, процес агрегації дозволяє отримати рівень обізнаності у сфері кібербезпеки для кожного окремого громадянина. Агрегована оцінка нормована $\vartheta(c_i) \in [0; 1]$, а коли $\vartheta(c_i) \to 1$, тоді це обумовлює високий рівень обізнаності громадянина c_i у сфері кібербезпеки.

Далі відбувається обчислення загального рівня обізнаності громадян у сфері кібербезпеки для досліджуваної території R. Не зменшуючи загальності, пропонується вивести середнє арифметичне агрегованих рівнів для досліджуваної території:

$$\vartheta_R = \frac{1}{n} \sum_{i=1}^{n} \vartheta(c_i). \quad (9)$$

Такий підхід дозволяє отримати узагальнену оцінку кіберобізнаності в регіональному або національному масштабі, що може бути використано для порівняльного аналізу, планування освітніх заходів чи оцінювання ефективності вже впроваджених ініціатив у сфері кібербезпеки.

На завершальному етапі відбувається виведення лінгвістичного рівня (LFC) обізнаності громадян у сфері кібербезпеки для досліджуваної території. Для цього отримані нормовані оцінки рівня ϑ_R зіставляються до одної змінної терм-множин $LFC = \{l_1; l_2; \dots; l_5\}$. Наприклад, $\vartheta_R \in (0{,}8;\ 1]$ – l_1 = “високий рівень”; $\vartheta_R \in (0{,}6;\ 0{,}8]$ – l_2= “рівень – вище середнього”; $\vartheta_R \in (0{,}4;\ 0{,}6]$ – l_3 = “середній рівень”; $\vartheta_R \in (0{,}2;\ 0{,}4]$ – l_4 = “низький рівень”; $\vartheta_R \in [0;\ 0{,}2]$ – l_5 = “дуже низький рівень”.

В результаті інтелектуальна модель уможливлює вивести знання, що відображають реальний стан обізнаності громадян у сфері кібербезпеки на певній території, виявити критичні зони з недостатнім рівнем знань, визначити основні прогалини у сприйнятті кіберризиків, а також сформувати обґрунтовані рекомендації для підвищення цифрової грамотності та розробки цільових інформаційно-просвітницьких кампаній.

Інтелектуальна модель оцінювання рівня обізнаності громадян у сфері кібербезпеки верифікована та апробовано на реальних даних населення Закарпатської області [11]. Протягом березня-червня 2025 року було здійснено анкетний збір даних від 315 респондентів по 49 запитань. Основна мета збору даних було спрямоване на вивчення ставлення до питань інформаційної безпеки у суспільстві. Отримані статистичні дані відповідають усім вимогам щодо формування вибірки. Це підтверджується тим, що обрані респонденти належать до повної групи елементів, що досліджуються та відповідають різноманітним демографічним характеристикам. Загалом, із 315 респондентів 60% є чоловіки, а 40% - жінки. Серед всіх респондентів 98,5% є люди працездатного віку, які активно взаємодіють з комп’ютерними інформаційними технологіями.

На повному наборі даних було виконано оцінювання рівня обізнаності громадян у сфері кібербезпеки, використовуючи розроблену інтелектуальну модель.

Було отримано вхідні дані використовуючи інформаційну модель. Фрагменти вхідних даних наведено в таблиці 1, а повний набір даних розміщено у відкритому доступі [11].

Таблиця 1

Фрагменти вхідних даних

Група критеріїв	Критерії	c_1	c_2	c_3	…	c_{315}
G_1	K_{11}	6	8	8	…	7
	K_{12}	7	5	8	…	2
	K_{13}	7	6	6	…	6
	K_{14}	7	8	3	…	2
	K_{15}	6	10	7	…	10
	K_{16}	6	8	7	…	7
	K_{17}	6	9	7	…	8
G_2	K_{21}	7	9	6	…	6
	K_{22}	7	8	7	…	8
	K_{23}	7	8	8	…	6
	K_{24}	6	9	10	…	6
	K_{25}	7	9	8	…	7
	K_{26}	8	9	7	…	8
G_3	K_{31}	8	9	4	…	6
	K_{32}	8	8	3	…	5
	K_{33}	7	7	7	…	2
	K_{34}	7	9	8	…	9
	K_{35}	7	8	4	…	9
G_4	K_{41}	3	4	2	…	1
	K_{42}	7	6	5	…	5
	K_{43}	4	8	3	…	5
	K_{44}	4	9	4	…	7

Після збору вхідних даних від респондентів необхідно перейти від кількісних бальних оцінок до нормованих значень. Для цього спочатку в межах кожної групи критеріїв обчислюється інтегральна оцінка $\delta_1(c_i)$, $\delta_2(c_i)$, $\delta_3(c_i)$, $\delta_4(c_i)$ згідно з формулою (2). Наступним етапом є фазифікація вхідних даних із застосуванням квадратичного S-сплайна для кожної з груп критеріїв. Функції належності $\mu_1(c_i)$, $\mu_2(c_i)$, $\mu_3(c_i)$, $\mu_4(c_i)$ розраховуються відповідно до формул (3)–(6). Отримані результати наведено в таблиці 2.

Таблиця 2

Фазифіковані вхідні дані

Група критеріїв	Значення	c_1	c_2	c_3	…	c_{315}
G_1	δ_1	45	54	46	…	42
	μ_1	0,7	0,883	0,725	…	0,621
G_2	δ_2	42	52	46	…	41
	μ_2	0,778	0,956	0,866	…	0,752
G_3	δ_3	37	41	26	…	31
	μ_3	0,851	0,934	0,456	…	0,665
G_4	δ_4	27	14	25	…	18
	μ_4	0,739	0,154	0,653	…	0,302

Далі фазифіковані вхідні дані обчислюються за згортковим методом для визначення агрегованого рівня обізнаності громадян у сфері кібербезпеки та загального рівня в межах досліджуваної території. Для цього ОПР задає вагові коефіцієнти для кожної групи критеріїв, наприклад: $v_1 = 9, v_2 = 8, v_3 = 10, v_4 = 9$. Далі знаходяться нормовані вагові коефіцієнти за формулою (7): w_1 =0,25; w_2 =0,22; w_3 =0,28; w_4 =0,25.

Далі відбувається відбувається перехід до агрегованого рівня обізнаності громадянина у сфері кібербезпеки за формулою (8): $\vartheta(c_1) = 0{,}66$; $\vartheta(c_2) = 0{,}877$; $\vartheta(c_3) = 0{,}538$; …; $\vartheta(c_{315}) = 0{,}583$.

Після цього відбувається обчислення загального рівня обізнаності громадян у сфері кібербезпеки для досліджуваної Закарпатської області, за формулою (9): ϑ_R =0,659. На завершальному етапі відбувається виведення лінгвістичного рівня (LFC) обізнаності громадян у сфері кібербезпеки, отримується: $\vartheta_R \in (0{,}6; 0{,}8]$ – l_2= “рівень – вище середнього”.

У результаті загальний рівень обізнаності громадян Закарпатської області у сфері кібербезпеки становив 0,659, що за лінгвістичною класифікацією відповідає рівню "вище середнього". Це свідчить про достатню, але не критично високу поінформованість населення з питань цифрової безпеки та підтверджує ефективність застосованої інтелектуальної моделі для аналізу подібних соціотехнічних характеристик.

Висновки з даного дослідження
і перспективи подальших розвідок у даному напрямі

У роботі представлено інтелектуальну модель оцінювання рівня обізнаності громадян у сфері кібербезпеки. Для цього: розроблено інформаційну модель оцінювання рівня обізнаності громадян у сфері кібербезпеки; розроблено згортковий метод визначення агрегованого рівня обізнаності громадян у сфері кібербезпеки та загального рівня в межах досліджуваної території; верифіковано та налаштовано інтелектуальну модель на реальних даних від 315 респондентів Закарпатської області; наведено приклади оцінювання.

Дослідження ґрунтується на використанні сучасного математичного апарату, зокрема теорії нечітких множин та інтелектуального аналізу знань. Застосування цього інструментарію дало змогу не лише адекватно формалізувати й кількісно оцінити рівень обізнаності громадян у сфері кібербезпеки, а й надати йому лінгвістичну інтерпретацію як на індивідуальному, так і на колективному рівні. Важливо, що даний підхід дозволяє враховувати суб'єктивні оцінки та нечіткість людських суджень, що є характерним для соціальних досліджень, де об’єктивні вимірювання не завжди можливі. Це значно підвищує достовірність і гнучкість моделі, а також сприяє прийняттю обґрунтованих управлінських рішень у сфері цифрової безпеки. Налаштування параметрів моделі здійснювалося на основі реальних соціологічних даних, зібраних безпосередньо серед респондентів, що забезпечило високу точність і релевантність отриманих результатів. Отримані висновки мають вагоме практичне значення для формування державної політики у сфері кібербезпеки, розробки інформаційно-просвітницьких програм, а також підвищення загального рівня цифрової обізнаності населення.

Обмеженням проведеного дослідження є вибірка респондентів у дослідницькій анкеті та територіальна прив’язаність до Закарпатської області. Також до обмежень можна віднести вибір типу функцій належності, що може призвести до неоднозначності у кінцевих результатів. Тим не менше, достовірність отриманих результатів підтверджується правильним використанням математичного інструментарію.

У майбутньому планується розширити дослідження на інші регіони України з метою отримання більш репрезентативної картини рівня обізнаності громадян у сфері кібербезпеки. Також передбачається створення програмного забезпечення, яке реалізуватиме інтелектуальну модель оцінювання, що дозволить використовувати її на практиці органам місцевого самоврядування, освітнім установам та іншим зацікавленим сторонам для ухвалення обґрунтованих рішень щодо підвищення цифрової грамотності населення.

Література

1. Taherdoost, H. Understanding cybersecurity frameworks and information security standards – A review and comprehensive overview. *Electronics*, 2022, 11(14), 2181. https://doi.org/10.3390/electronics11142181
2. Tolah, A., Furnell, S. M., Papadaki, M. An empirical analysis of the information security culture key factors framework. *Computers & Security*, 2021, 108, 102354. https://doi.org/10.1016/j.cose.2021.102354
3. Almansoori, A., Al-Emran, M., Shaalan, K. Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences*, 2023, 13(9), 5700. https://doi.org/10.3390/app13095700
4. Spruit, M., Oosting, D., Kreffer, C. Factors that influence secure behaviour while using mobile digital devices. *Information and Computer Security*, 2024, 32(5), pp. 729–747. https://doi.org/10.1108/ICS-02-2024-0035
5. Nawawi, A., Puteh Salin, A. S. Employee fraud and misconduct: Empirical evidence from a telecommunication company. *Information and Computer Security*, 2018, 26(1), pp. 129–144. https://doi.org/10.1108/ICS-07-2017-0046
6. Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., von Solms, B. Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security*, 2022, 119, 102756. https://doi.org/10.1016/j.cose.2022.102756
7. Федушко, С. Сучасні підходи до дослідження кібербезпеки та кібергігієни в умовах цифрової трансформації суспільства. *Herald of Khmelnytskyi National University. Technical Sciences*, 2023, 321(3), pp. 210–213. https://doi.org/10.31891/2307-5732-2023-321-3-210-213
8. Білявська, Ю., Шестак, Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Товари і ринки*, 2022, № 3, с. 47–59. http://nbuv.gov.ua/UJRN/tovary_2022_3_6
9. Bognár, L., Bottyán, L. Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences*, 2024, 14(6), 588. https://doi.org/10.3390/educsci14060588
10. Kelemen, M., Polishchuk, V., Gavurová, B., Andoga, R., Szabo, S., Yang, W., Christodoulakis, J., Gera, M., Kozuba, J., Kaľavský, P., Antoško, M. Educational model for evaluation of airport NIS security for safe and sustainable air transport. *Sustainability*, 2020, 12, 6352. https://doi.org/10.3390/su12166352

11. Дані 315 респондентів для оцінювання рівня обізнаності громадян у сфері кібербезпеки. URL: https://docs.google.com/spreadsheets/d/12XNBLXmqqNghlYmq9utLcQSOAvuuKRCv/edit?usp=sharing&ouid=111497346858387909549&rtpof=true&sd=true (дата звернення: 23.07.2025).

References

1. Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards – A review and comprehensive overview. *Electronics*, 11(14), 2181. https://doi.org/10.3390/electronics11142181

2. Tolah, A., Furnell, S. M., & Papadaki, M. (2021). An empirical analysis of the information security culture key factors framework. *Computers & Security*, 108, 102354. https://doi.org/10.1016/j.cose.2021.102354

3. Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences*, 13(9), 5700. https://doi.org/10.3390/app13095700

4. Spruit, M., Oosting, D., & Kreffer, C. (2024). Factors that influence secure behaviour while using mobile digital devices. *Information and Computer Security*, 32(5), 729–747. https://doi.org/10.1108/ICS-02-2024-0035

5. Nawawi, A., & Puteh Salin, A. S. (2018). Employee fraud and misconduct: Empirical evidence from a telecommunication company. *Information and Computer Security*, 26(1), 129–144. https://doi.org/10.1108/ICS-07-2017-0046

6. Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security*, 119, 102756. https://doi.org/10.1016/j.cose.2022.102756

7. Fedushko, S. (2023). Suchasni pidkhody do doslidzhennya kiberbezpeky ta kiberhihiyeny v umovakh tsyfrovoyi transformatsiyi suspil′stva. *Herald of Khmelnytskyi National University. Technical Sciences*, 321(3), 210–213. https://doi.org/10.31891/2307-5732-2023-321-3-210-213

8. Bilyavs′ka, YU., & Shestak, YA. (2022). Kiberbezpeka ta kiberhihiyena: nova era tsyfrovykh tekhnolohiy. *Tovary i rynky*, (3), 47–59. http://nbuv.gov.ua/UJRN/tovary_2022_3_6

9. 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), 588. https://doi.org/10.3390/educsci14060588

10. Kelemen, M., Polishchuk, V., Gavurová, B., Andoga, R., Szabo, S., Yang, W., Christodoulakis, J., Gera, M., Kozuba, J., Kaľavský, P., & Antoško, M. (2020). Educational model for evaluation of airport NIS security for safe and sustainable air transport. *Sustainability*, 12, 6352. https://doi.org/10.3390/su12166352

11. Data from 315 respondents to assess the level of awareness of citizens in the field of cybersecurity. Retrieved from: https://docs.google.com/spreadsheets/d/12XNBLXmqqNghlYmq9utLcQSOAvuuKRCv/edit?usp=sharing&ouid=111497346858387909549&rtpof=true&sd=true. (Date of access: 23.07.2025).