

FUZZY MODEL FOR ASSESSING DIGITAL SECURITY LITERACY ACROSS POPULATION GROUPS WITH DIFFERENT SOCIAL PROFILES

Volodymyr Polishchuk^{1,2}, Vasyl Sehlianyk², Inna Polishchuk^{1,2}, Andrii Shafar²

¹Technical University of Kosice, Department of Flight Training, Kosice, Slovak Republic, ²Uzhhorod National University, Department of Software Systems, Uzhhorod, Ukraine

Abstract. The article proposes a fuzzy model for assessing the level of digital security literacy of the population, considering socio-demographic characteristics. The relevance of the study is determined by the growth of cyber threats, digital risks, and the role of the human factor in ensuring the stability of the digital environment, which requires a transition from fragmentary measurements to comprehensive and interpretable assessment approaches. The scientific novelty of the work lies in combining the convolution method and fuzzy modelling to form integral quantitative and linguistic assessments of digital security literacy across various social profiles of the population. The proposed method makes it possible to formalize heterogeneous demographic and behavioural data, conduct profile-based analysis, and generate targeted analytical conclusions to support management decision-making. The practical significance of the study was confirmed by verifying the proposed method on real empirical data obtained from a questionnaire survey of 315 respondents in the Transcarpathian region. The verification showed that the proposed method provides a normalized quantitative assessment for a selected social profile with an integral value of 0.644, which corresponds to an above-average level of digital security literacy. Compared with simple averaging of the entire sample, the proposed method increases the analytical specificity of the assessment by enabling profile-oriented evaluation and targeted interpretation of results rather than only obtaining a generalized population-level indicator. The results obtained demonstrate the possibility of using the proposed method to assess the level of digital security literacy, segment the population by social profiles, identify vulnerable groups, and justify targeted educational and preventive measures. Prospects for further research are related to expanding the empirical base, automating data collection and processing procedures, integrating new assessment criteria, and analysing the dynamics of digital security literacy over time and across regions.

Keywords: digital security, personal data, cyber awareness, decision support, fuzzy modelling, digital risk management

MODEL ROZMYTY DO OCENY POZIOMU KOMPETENCJI W ZAKRESIE BEZPIECZEŃSTWA CYFROWEGO W POPULACJACH O RÓŻNYCH PROFILACH SPOŁECZNYCH

Streszczenie. W artykule zaproponowano model rozmyty służący do oceny poziomu kompetencji społeczeństwa w zakresie bezpieczeństwa cyfrowego, uwzględniający cechy społeczno-demograficzne. Znaczenie niniejszego badania wynika z nasilenia się cyberzagrożeń i ryzyka cyfrowego oraz roli czynnika ludzkiego w zapewnianiu stabilności środowiska cyfrowego, co wymaga przejścia od fragmentarycznych pomiarów do kompleksowych i interpretowalnych metod oceny. Nowość naukowa pracy polega na połączeniu metody splotu i modelowania rozmytego w celu stworzenia integralnych ocen ilościowych i językowych poziomu wiedzy z zakresu bezpieczeństwa cyfrowego w różnych profilach społecznych ludności. Proponowana metoda umożliwia sformalizowanie heterogenicznych danych demograficznych i behawioralnych, przeprowadzenie analizy opartej na profilach oraz sformułowanie ukierunkowanych wniosków analitycznych wspierających proces podejmowania decyzji zarządczych. Praktyczne znaczenie badania potwierdzono poprzez weryfikację proponowanej metody na rzeczywistych danych empirycznych uzyskanych w wyniku ankiety przeprowadzonej wśród 315 respondentów w regionie Zakarpacia. Weryfikacja wykazała, że proponowana metoda zapewnia znormalizowaną ocenę ilościową dla wybranego profilu społecznego o wartości integralnej wynoszącej 0,644, co odpowiada ponadprzeciętnemu poziomowi kompetencji w zakresie bezpieczeństwa cyfrowego. W porównaniu z prostym uśrednieniem całej próby proponowana metoda zwiększa specyfikę analityczną oceny, umożliwiając ocenę zorientowaną na profil oraz ukierunkowaną interpretację wyników, a nie tylko uzyskanie uogólnionego wskaźnika na poziomie populacji. Uzyskane wyniki wskazują na możliwość wykorzystania proponowanej metody do oceny poziomu kompetencji w zakresie bezpieczeństwa cyfrowego, segmentacji populacji według profili społecznych, identyfikacji grup szczególnie narażonych oraz uzasadnienia ukierunkowanych działań edukacyjnych i prewencyjnych. Perspektywy dalszych badań wiążą się z poszerzeniem bazy empirycznej, automatyzacją procedur gromadzenia i przetwarzania danych, włączeniem nowych kryteriów oceny oraz analizą dynamiki kompetencji w zakresie bezpieczeństwa cyfrowego w czasie i w różnych regionach.

Słowa kluczowe: cyfrowe bezpieczeństwo, dane osobowe, świadomość cyberbezpieczeństwa, wspomaganie podejmowania decyzji, modelowanie rozmyte, zarządzanie ryzykiem cyfrowym

Introduction

The rapid digitalization of society, the expansion of electronic services, and the growing dependence of socio-economic processes on information and communication technologies make the problem of ensuring digital security at the individual, community, and national levels more urgent. The increase in cyber threats, the spread of fraudulent schemes, leaks of personal data, and the spread of manipulative information necessitate an appropriate level of population literacy in digital security as a key prerequisite for the sustainable development of a digital society [8, 9].

The relevance of this study is consistent with the plan's development of the European Union, with strategic documents in the field of digital transformation and cybersecurity, which determine the improvement of digital competences of citizens, the development of a safe digital environment, and strengthening trust in digital services [8, 10]. The Digital Decade 2030 program emphasizes the need to achieve a high level of digital skills in the population and increase the cyber resilience of society as the basis for a competitive and inclusive economy [10].

In addition, the research issues directly correlate with the Sustainable Development Goals defined by the UN Agenda 2030, particularly those aimed at ensuring quality education, developing innovation and infrastructure, reducing social

inequality, and forming effective and accountable institutions [18, 19]. Increasing the population's literacy in digital security contributes to expanding access to digital opportunities, reducing the digital divide between social groups, and strengthening trust in digital technologies [6, 7].

In this context, the development of intellectual-analytical tools that can provide a comprehensive, flexible, and interpretable assessment of the population's literacy level in digital security, considering socio-demographic characteristics, is of particular importance. The proposed research aims to develop a scientifically sound approach to such an assessment that can serve as an analytical basis for decision-making, targeted educational program development, and the implementation of strategies for sustainable digital development.

The main goal of the scientific research is to develop a fuzzy model for assessing the literacy levels of populations with different social profiles in the field of digital security.

1. Literature review

The digitalization of society and the rapid spread of online services are accompanied by an increase in cyber threats, fraud, and the risk of personal data leakage, making digital security a key factor in sustainable development. Under these conditions, the literacy of the population in the field of digital security

becomes particularly important, since it is the human factor that often determines the level of vulnerability of the digital environment.

Modern scientific research confirms the need to measure not only knowledge but also users' behavioural practices, motivational and contextual factors, as well as to consider differences across socio-demographic groups. In this regard, the review of relevant sources is aimed at generalizing approaches to assessing cyber awareness and substantiating the need for integrated intellectual-analytical tools for diagnosing the level of digital security literacy of the population and forming targeted recommendations.

Taha and Dahabiyeh investigated students' level of information security awareness and compared the results by device type (smartphones vs. computers). The findings confirm that security behavioural patterns and risk sensitivity vary across digital contexts, and therefore literacy assessments should be tailored to specific technology use scenarios [17].

In his work, Alqahtani empirically analysed the factors influencing students' cybersecurity awareness and highlighted the importance of emphasizing thematic domains (password hygiene, browser security, social media security). Such structuring is methodologically helpful in forming a system of criteria and building a multidimensional model, where the integral assessment is decomposed into interpretable components [1].

Rohan, Pal, Hautamäki et al. conducted a systematic review of scales used to measure information security awareness. They found widespread gaps in psychometric validation (incomplete substantiation of validity, construct heterogeneity, and limited reproducibility). This result argues for transparent calculation procedures and a standardized approach to indicator interpretation within an intelligence analytics platform [16].

Bognár and Bottyán developed and validated a personal cyber-awareness assessment tool that focuses not only on knowledge but also on actual online safety practices. This is important for population literacy studies, as it confirms the feasibility of combining cognitive (knowledge/understanding) and behavioural (actions/habits) indicators in a single assessment framework [5].

In their study, Argyridou, Nifakos, Laoudias et al. proposed a methodology to improve cyber hygiene and data privacy awareness in organizations, emphasizing the connection between survey results, risk interpretation, and the formulation of practical interventions (e.g., educational activities, policies, controls). For your platform, this is an example of how literacy measurement can be translated into guided recommendations for target groups [3]. Barakovic et al. investigated cyber hygiene knowledge, awareness, and behavioural practices in a university environment and identified typical weaknesses that require targeted educational interventions. The findings reinforce the need to segment results and move from "average" to profile analysis to identify the most vulnerable groups [4].

Rizal and Setiawan have summarized approaches to measuring cybersecurity awareness by analysing the "focus areas" of assessment tools. They emphasize that the validity of an instrument largely depends on the structure of the criteria and the completeness of coverage of key digital security domains, which is methodologically relevant for constructing the questionnaire and the knowledge base of your platform [15].

Prümmer, van Steen, and van den Berg systematized modern cyber-learning methods, their effectiveness, and showed that the positive effects of training are often observed at the level of knowledge/attitudes, while long-term behavioural changes are less frequently confirmed. This argues for the need for platforms that provide not a one-time measurement but repeated assessments and analyses of the dynamics of change after interventions [13]. In another work, in a further study (meta-analysis), it was found that the effect of training is statistically more noticeable for behavioural predictors (knowledge, attitude, self-efficacy) than for users' actual behaviour. For intellectual-analytical assessment, this means the feasibility of distinguishing between "declared readiness" and "behavioural implementation"

and forming different types of recommendations for each level [14].

Alqarni investigated the relationship between cyber awareness and data protection behaviour among high school students, showing that threat perception serves as a mediator and that the intensity of Internet use acts as a moderator. These results confirm the importance of accounting for psychological and contextual variables when assessing digital security literacy, as well as the feasibility of multilevel modelling within the platform [2]. The reviewed studies confirm the relevance of measuring digital/cybersecurity literacy. Still, most of the work focuses on separate environments (mainly educational institutions or organizations) or on isolated aspects (cyber hygiene, separate scales, training effectiveness). At the same time, the scientific literature lacks comprehensive approaches that simultaneously combine: (1) representative data collection for different social profiles, (2) transparent and reproducible procedures for integral assessment, (3) interpretable classification of results, and (4) the formation of targeted recommendations and monitoring changes over time. It is this gap that justifies the lack of such studies in a completed form and confirms the scientific and practical relevance of the proposed approach (Figure 1).

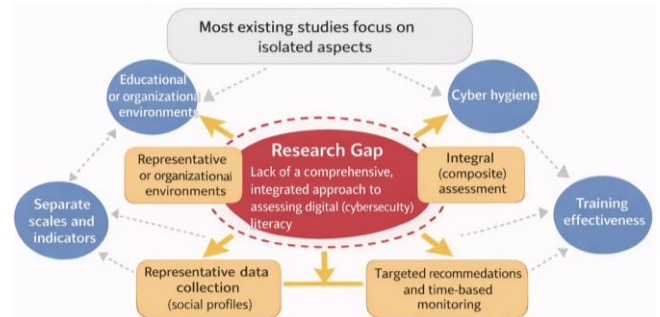


Fig. 1. Research gap in measuring digital cyberliteracy

2. Materials and methods

The study is conducted in a particular territory R , which can represent a city, region, or country. The population of this territory is denoted as $C = \{c_1; c_2; \dots; c_n\}$. Various demographic characteristics are considered for citizens, forming a social profile $SP = \{sp_1; sp_2; \dots; sp_k\}$. It is necessary to assess the level of literacy in digital security within a specific territory across various social profiles.

To obtain input data, a survey is conducted. Input information is collected using a text questionnaire developed based on a system of criteria K , which are combined into groups G . Using the previously developed convolutional method, the aggregated level of citizens' awareness in cybersecurity ($\theta(c)$) and the general level within the studied territory – M_S [11] are determined. After that, the obtained data are analysed using a fuzzy model to assess the level of literacy of populations with different social profiles in the field of digital security – M_{DS} .

The formal formulation of a scientific study assessing the literacy levels of populations with different social profiles in the field of digital security can be represented as an operator:

$$M(R, C, SP, \theta(c), M_{DS}) | Y(f) \quad (1)$$

The operator M_3 , based on the input data $R, C, SP, \theta(c)$, matches the output value $Y(f_3) = \{m_{dsp}(sp); DSP\}$, which consists of the following quantities: $m_{dsp}(sp)$ – quantitative level of literacy of the population in the field of digital security of a particular social profile (sp); DSP – linguistic level of literacy of the population in the field of digital security.

For a visual presentation of the study, a structural diagram of the fuzzy model is provided (Figure 2).

Figure 2 reflects the platform's structural diagram and illustrates the interaction logic of its main functional modules during data processing, analysis, and interpretation. The structural diagram demonstrates the sequence of information

flows from collecting input data through surveying respondents and building a database to the application of the convolutional method and a fuzzy evaluation model. Based on the results of analytical processing, a knowledge base is formed to support decision-making procedures. The final stage of the platform is the formation of initial quantitative and linguistic assessments of the population's literacy in digital security, with the possibility of their review and correction by the decision-maker (DM). Thus, the structural diagram presented in Figure 2 reflects a holistic cycle of intellectual-analytical evaluation and emphasizes the systemic nature of the proposed platform.

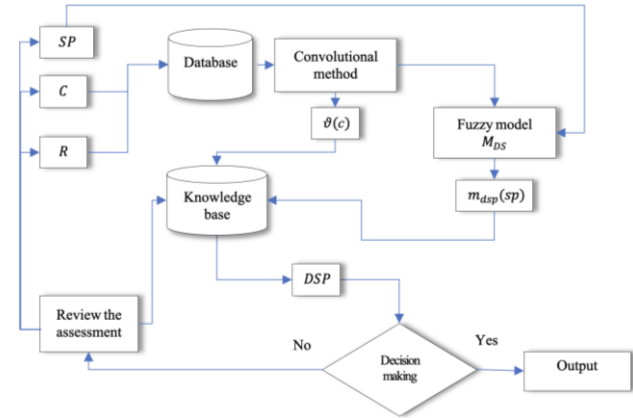


Fig. 2. Structural diagram of the intellectual-analytical platform

At the first stage, using the developed convolutional method (M_S), the levels of citizens' cybersecurity awareness are calculated: $\{\vartheta(c_1); \vartheta(c_2); \dots; \vartheta(c_n)\}$ [11]. The value $\vartheta(c)$ was obtained as an aggregated indicator of an individual citizen's awareness in the field of cybersecurity. It is calculated by combining the respondent's answers to a structured set of cybersecurity-related questions into a normalized integral value, which reflects the general level of awareness, knowledge, and behavioural readiness of a citizen in typical digital security situations. In the present study, this value is used as an input indicator for further assessment of digital security literacy within selected social profiles.

Next, a fuzzy model for assessing the literacy level of populations with different social profiles in the field of digital security is presented – M_{DS} .

Let citizen C have different demographic characteristics $S = \{s_1; s_2; \dots; s_m\}$, which form a certain social profile $SP = \{sp_1; sp_2; \dots; sp_k\}$. The characteristics of citizens have both quantitative and qualitative aspects. Therefore, to ensure correct comparison and further analytical processing, it is advisable to formalize demographic indicators and bring them to a single normalized scale. In this context, formalized answer options are defined for each characteristic, along with appropriate normalization methods. Within the framework of this study, the following demographic characteristics are proposed:

- $s_1(t_1)$ – gender.

The score is determined – $t_1 = \{\text{man; woman}\}$ and formalizes:

$$sp_1(t_1) = \begin{cases} 1 & \text{if } t_1 = \text{"man"} \\ 0 & \text{if } t_1 = \text{"woman"} \end{cases} \quad (2)$$

- $s_2(t_2)$ – age.

The age of citizens is estimated in years $t_2 \in [18; 99]$. To formalize this indicator, it is proposed to use the corresponding characteristic function:

$$sp_2(t_2) = \begin{cases} 0.2 & \text{if } t_2 = \text{"from 18 to 25"} \\ 0.3 & \text{if } t_2 = \text{"from 26 to 34"} \\ 0.4 & \text{if } t_2 = \text{"from 35 to 42"} \\ 0.5 & \text{if } t_2 = \text{"from 43 to 50"} \\ 0.6 & \text{if } t_2 = \text{"from 51 to 58"} \\ 0.7 & \text{if } t_2 = \text{"from 59 to 66"} \\ 0.8 & \text{if } t_2 = \text{"from 67 to 74"} \\ 0.9 & \text{if } t_2 = \text{"from 75 to 82"} \\ 1 & \text{if } t_2 = \text{"from 83 to 99"} \end{cases} \quad (3)$$

- $s_3(t_3)$ – primary socioeconomic status.

Primary socio-economic status is an important characteristic that reflects a person's basic life conditions and position in society's socio-economic structure. To consider the influence of this factor within the framework of the study, it is formalized using the appropriate characteristic function:

$$sp_3(t_3) = \begin{cases} 0.1 & \text{if } t_3 = \text{"Student"} \\ 0.2 & \text{if } t_3 = \text{"Employed"} \\ 0.4 & \text{if } t_3 = \text{"Unemployed"} \\ 0.6 & \text{if } t_3 = \text{"Pregnancy/care"} \\ 0.8 & \text{if } t_3 = \text{"Pensioner"} \\ 1 & \text{if } t_3 = \text{"Person with special needs"} \end{cases} \quad (4)$$

- $s_4(t_4)$ – highest completed education.

The level of education is one of the key socio-economic indicators that determines a person's knowledge, skills, and ability to interact effectively with the digital environment. To quantitatively take this factor into account in the model, it is formalized by applying the appropriate characteristic function:

$$sp_4(t_4) = \begin{cases} 0.2 & \text{if } t_4 = \text{"Completed general secondary education"} \\ 0.4 & \text{if } t_4 = \text{"Vocational and technical education"} \\ 0.6 & \text{if } t_4 = \text{"Higher education level I"} \\ 0.8 & \text{if } t_4 = \text{"Higher education level II"} \\ 1 & \text{if } t_4 = \text{"Higher education level III (PhD)"} \end{cases} \quad (5)$$

- $s_5(t_5)$ – average net monthly income.

Average net monthly income is an essential socio-economic indicator that characterizes a person's financial capabilities and their access to resources and services. To quantitatively account for this indicator's impact within the study's framework, it is formalized using the appropriate characteristic function:

$$sp_5(t_5) = \begin{cases} 0.1 & \text{if } t_5 = \text{"to 10000 UAH"} \\ 0.2 & \text{if } t_5 = \text{"10000 – 14000 UAH"} \\ 0.4 & \text{if } t_5 = \text{"14000 – 18000 UAH"} \\ 0.6 & \text{if } t_5 = \text{"18000 – 22000 UAH"} \\ 0.8 & \text{if } t_5 = \text{"22000 – 30000 UAH"} \\ 1 & \text{if } t_5 = \text{"more 30000 UAH"} \end{cases} \quad (6)$$

- $s_6(t_6)$ – marital status.

Marital status reflects the social conditions of a person's life and can affect the level of responsibility, social support, and behavioural characteristics. To take this factor into account in the model, it is formalized using the appropriate characteristic function:

$$sp_6(t_6) = \begin{cases} 0.4 & \text{if } t_6 = \text{"single / unmarried"} \\ 0.6 & \text{if } t_6 = \text{"married"} \\ 0.8 & \text{if } t_6 = \text{"divorced"} \\ 1 & \text{if } t_6 = \text{"widower / widow"} \end{cases} \quad (7)$$

This study aims to determine the level of digital security literacy of the population across different social profiles, $SP = \{sp_1; sp_2; \dots; sp_k\}$. A social profile is formed by grouping different demographic characteristics S by specifying some DM rule – τ .

The formation of a social profile $SP(\tau)$ of citizens to assess the level of literacy in the field of digital security in accordance with the rules of the decision-maker (τ), is defined in the study as a "target need". In other words, the vector of target needs of a particular social profile is a set of demographic characteristics of a conditional group of citizens who form the corresponding social profile, and for whom it is necessary to determine the level of literacy in the field of digital security for the purpose of further analysis and development of decision-making support scenarios.

Let the obtained normalized data on citizens C , formed according to their demographic characteristics in the studied region R , be presented in the form of a decision matrix:

$$SPC = \begin{pmatrix} sp_1(c_1) & sp_1(c_2) & \dots & sp_1(c_n) \\ sp_2(c_1) & sp_2(c_2) & \dots & sp_2(c_n) \\ \dots & \dots & \dots & \dots \\ sp_k(c_1) & sp_k(c_2) & \dots & sp_k(c_n) \end{pmatrix} \quad (8)$$

In the next step, the decision maker introduces a k -dimensional vector of target needs to assess the level of digital

security literacy of a particular social profile. This vector is used to formalize the requirements for the corresponding profile and is hereinafter denoted as $Z(\tau) = Z^*(\overline{sp}_1; \overline{sp}_2; \dots; \overline{sp}_k)$.

Next, an approach is proposed to rank citizens, $C = \{c_1, c_2, \dots, c_n\}$, in which the first positions are occupied by alternatives that most closely correspond to the given vector of "target needs" for a specific social profile. The main idea of the approach is to find a solution that, in terms of the set of demographic characteristics, is as close as possible to the specified vector.

For this purpose, the SPC matrix and the $Z(\tau)$ vector are used to determine a set of indicators that reflect the degree of proximity of the elements of the SPC matrix to the corresponding components of the "target needs" vector of a particular social profile:

$$q_{ui} = 1 - \frac{|\overline{sp}_u - sp_u(c_i)|}{\max\{\overline{sp}_u - \min(sp_u(c_i)), \max(sp_u(c_i)) - \overline{sp}_u\}} \quad (9)$$

$$u = \overline{1, k}; i = \overline{1, n}$$

The formed matrix $Q = \{q_{ui}\}$ reflects the relative estimates of the proximity of citizens c_i to the vector of target needs Z^* for each demographic characteristic. It should be noted that the decision-maker is not obliged to include all demographic indicators in the vector of target needs. In the case of choosing a limited set of characteristics, the SPC decision matrix will accordingly have a reduced number of rows.

At the next stage, the decision maker sets the weight coefficients $\{v_1, v_2, \dots, v_k\}$ for each demographic characteristic of the social profile SP , for example, within the interval $[1; 10]$. To ensure comparability of the indicators, the weight coefficients are normalized:

$$w_u = \frac{v_u}{\sum_{u=1}^k v_u}, u = \overline{1, k}; w_u \in [0; 1] \quad (10)$$

Such normalization makes it possible that $\sum_{u=1}^k w_u = 1$.

At the final stage, a ranking series of citizens, $C = \{c_1, c_2, \dots, c_n\}$, is formed with respect to the "target needs" of a given social profile. Without limiting the generality of the approach, a convolution method is used to aggregate partial estimates, particularly an average convolution, which has the following form:

$$\rho(c_i) = \sum_{u=1}^k w_u \cdot q_{ui} \quad (11)$$

Next, the quantitative literacy level of the population in the field of digital security for a given social profile is derived. Let the DM specify the number of citizens r ($r < n$) from the studied social profile to derive the level of literacy in the field of digital security on their basis. Then the first r citizens ($A_1, A_2, \dots, A_r$) from the constructed ranking series $A = (A_1, A_2, \dots, A_n)$, are selected for consideration, based on the estimates $\rho(c_i)$. Using the aggregated level of awareness of citizens in the field of cybersecurity ($\vartheta(c)$) the average value is calculated:

$$m_{dsp}(sp) = \frac{1}{r} \sum_{d=1}^r \vartheta(c_d) \quad (12)$$

When $m_{dsp}(sp) \rightarrow 1$ then there will be a high level of literacy of the population in the field of digital security of the selected social profile.

As a result, a set of citizens was selected whose demographic characteristics most closely match the decision-maker's social profile. Based on the sample, the average level of literacy in digital security was further calculated.

To derive the complex linguistic assessment of digital security literacy for a selected social profile, the normalized quantitative value $m_{dsp}(sp) \in [0; 1]$ is mapped onto an ordered set of linguistic terms $DSP = \{dsp_1, dsp_2, dsp_3, dsp_4, dsp_5\}$. This mapping is formalized by the linguistic assessment function:

$$L_{DSP}: m_{dsp}(sp) \rightarrow DSP \quad (13)$$

$$L_{DSP}(m_{dsp}(sp)) = \begin{cases} dsp_1, & 0.7 < m_{dsp}(sp) \leq 1 \\ dsp_2, & 0.6 < m_{dsp}(sp) \leq 0.7 \\ dsp_3, & 0.5 < m_{dsp}(sp) \leq 0.6 \\ dsp_4, & 0.3 < m_{dsp}(sp) \leq 0.5 \\ dsp_5, & 0 \leq m_{dsp}(sp) \leq 0.3 \end{cases} \quad (14)$$

where $dsp_1, dsp_2, dsp_3, dsp_4$, and dsp_5 correspond respectively to high, above-average, average, low, and very low levels of digital security literacy. Therefore, the linguistic assessment is obtained through a formal interval-based classification of the normalized quantitative indicator.

As a result, the fuzzy model enables the derivation of knowledge characterizing the level of digital security literacy of citizens within a defined social profile. Such knowledge is essential for state authorities and public administration institutions, as it provides an analytical basis for developing targeted educational programs, formulating digital security policies, prioritizing resources, and anticipating risks in the digital environment.

3. Results

The fuzzy model for assessing the level of population literacy in digital security was verified and based on real population data from the Transcarpathian region [12]. During March–June 2025, a questionnaire survey was conducted, within the framework of which empirical data were collected from 315 respondents on 49 questions. The study aimed to analyse the population's attitude toward information security problems and identify the features of their interaction with the digital environment. The obtained statistical data meet the requirements for sample representativeness, as confirmed by the respondents' membership in the target population and the diversity of their socio-demographic characteristics. In the sample structure, 60% are men and 40% are women; at the same time, 98.5% of the respondents are of working age and actively use computer information technologies.

The main goal of data collection was to establish a reliable empirical basis for assessing the level of literacy of the population in digital security, as well as to identify features of risk perception, behavioural practices, and citizens' awareness of information security threats in the digital environment. The data obtained were necessary for further verification of the developed intellectual-analytical platform, conducting quantitative and linguistic analyses of the results, and substantiating management decisions aimed at increasing the digital security of various social profiles of the population.

The developed technology was verified on the complete set of collected data. To ensure the reproducibility of experimental results by other researchers, an example of the evaluation procedure is provided.

Separate fragments of input data on demographic characteristics S and their normalized values SP (according to formulas (2)–(7)), as well as the aggregated level of citizens' awareness in the field of cybersecurity ($\vartheta(c)$) are presented in Table 1, while the complete set of data is publicly available [12].

Let the DM set a rule for entering a "target need" for all demographic characteristics: $\tau = \{\text{male; from 18 to 25; Student; Higher education level I (bachelor); up to 10,000 UAH; single}\}$. Then the vector of "target needs" will have the form $Z(\tau) = Z^*(1; 0.2; 0.1; 0.6; 0.1; 0.4)$.

Using formula (9), the calculation of the relative indicators of the proximity of citizens to the vector of "target needs" of a certain social profile Z^* for each demographic characteristic is carried out. As a result, a matrix of dimension 315×6 , is formed, while its fragment corresponding to citizens $c_1, c_2, \dots, c_{315}$, has the following form:

$$Q = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0.75 & 1 & \dots & 1 \\ 0.889 & 1 & \dots & 0.444 \\ 0 & 1 & \dots & 1 \\ 0.667 & 1 & \dots & 1 \\ 0.667 & 1 & \dots & 0.667 \end{pmatrix}$$

The DM determines a system of weight coefficients, the values of which belong to the interval $[1; 10]$, for each demographic characteristic of the corresponding social profile:

$v_1=5, v_2=7, v_3=9, v_4=9, v_5=7, v_6=6$. At the next stage, the normalized weight coefficients are calculated according to formula (10): $w_1=0.12, w_2=0.16, w_3=0.21, w_4=0.21, w_5=0.16, w_6=0.14$.

After that, according to formula (11), a convolutional approach is applied to form a ranking series of citizens according to the degree of compliance with "target needs": $\rho(c_1)=0.627, \rho(c_2)=0.88, \dots, \rho(c_{315})=0.717$.

Table 1. Demographic data snippets

Demographic characteristics	c_1	c_2	c_3	...	c_{315}
s_1	t_1	Man	Woman	...	Woman
	sp_1	1	0	...	0
s_2	t_2	38	19	...	24
	sp_2	0.4	0.2	...	0.2
s_3	t_3	Employed	Student	...	Maternity/paternity leave
	sp_3	0.2	0.1	...	0.6
s_4	t_4	higher education level III (PhD)	higher education level I	...	higher education level I
	sp_4	1	0.6	...	0.6
s_5	t_5	14000 – 18000 UAH	to 10000 UAH	...	to 10000 UAH
	sp_5	0.4	0.1	...	0.1
s_6	t_6	married	single / unmarried	...	married
	sp_6	0.6	0.4	...	0.6
Aggregated level of awareness	$\vartheta(c)$	0.66	0.877	...	0.583

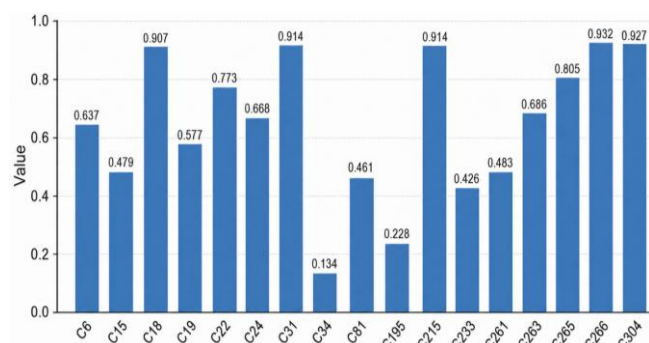


Fig. 3. The value of the aggregate level of awareness of the first 17 citizens

Using the aggregated level of awareness of citizens in the field of cybersecurity ($\vartheta(c)$), the average value is determined according to the formula (12):

$$m_{dsp}(sp) = \frac{1}{17}(0.637+0.479+\dots+0.927) = 0.644$$

Since the obtained value $m_{dsp}(sp) \in (0.6; 0.7]$, for the studied social profile $\tau=\{\text{male; from 18 to 25; Student; Higher education 1st level (bachelor); up to 10,000 UAH; single}\}$, a linguistic assessment $dsp_2 = \text{"The level of literacy of the population in the field of digital security is above average"}$ is established.

Thus, the results of the experimental study confirmed the efficiency and adequacy of the developed fuzzy model for assessing the level of population literacy in digital security. Based on real empirical data, a ranking series of citizens was formed, and the quantitative and linguistic levels of digital security literacy for a given social profile were determined. The obtained value of the integral indicator indicates that the population's literacy level exceeds the average. It confirms the platform's practical application for analysis and support of management decisions in the field of digital security across various social groups.

4. Discussion

The proposed fuzzy model for assessing the level of population literacy in digital security offers several significant advantages over traditional approaches to analysing similar social and informational phenomena. First, its key feature is the combination of convolutional methods with fuzzy modelling, which enables effective handling of heterogeneous

data that are both quantitative and qualitative. This is fundamentally important for research in digital security, where a significant portion of the information is based on subjective assessments, behavioural characteristics, and levels of risk awareness. The model's advantages also include its flexibility and adaptability. The concept of "target social profile" enables the DM to develop different analysis scenarios based on the demographic, socio-economic, or other characteristics of the population. Unlike classical statistical methods, which are usually focused on averaged indicators across the entire sample, the proposed approach allows differentiated results for individual population groups, thereby significantly increasing the practical value of the knowledge obtained for the formation of state policy and targeted educational programs.

Compared to standard methods of assessing digital or information literacy, which rely on simple indices, scale scores, or regression analysis, the developed model provides a deeper interpretation of the results. In particular, the use of fuzzy term sets allows combining quantitative assessments with linguistic conclusions, facilitating the perception of results not only for researchers but also for representatives of public administration bodies. At the same time, classical index approaches, although more straightforward to implement, often fail to account for data uncertainty and are limited to rigid threshold values, leading to simplified or insufficiently accurate conclusions.

However, the study has several limitations that must be considered when interpreting the results. Firstly, the empirical base is based on a questionnaire survey, which assumes the subjectivity of respondents' answers and the potential influence of socially desirable behaviour. Secondly, the study's results reflect the situation at a given point in time and may change as digital technologies continue to evolve and new threats to information security emerge. Thirdly, the choice of demographic characteristics and weighting factors partly depends on expert decisions, which, on the one hand, ensure the model's flexibility, but on the other hand, may affect the reproducibility of results across different conditions or regions.

Thus, the proposed fuzzy models are an effective tool for a comprehensive assessment of the level of literacy of the population in the field of digital security; however, its further development should be directed towards expanding the empirical base, automating the procedures for forming weighting factors, and adapting the model to the analysis of temporal changes. This will increase the accuracy of the assessment and expand the scope of practical application of the obtained results.

5. Conclusions

The main goal of the research is to develop an fuzzy model for assessing the literacy levels of populations with different social profiles in the field of digital security.

For the first time, a fuzzy model has been developed to assess the literacy level of populations with different social profiles in the field of digital security. Six demographic characteristics have been proposed for forming a social profile. The concept of "target needs" for DM for a specific social profile has been introduced. The output is a normalized quantitative measure of literacy in the field of digital security for the population with a specific social profile, as well as the linguistic level of literacy of the population in that field.

Prospects for further research include the development of software support for the intellectual-analytical platform, which will automate data collection, processing, and visualization. In addition, it is planned to expand the functionality of the platform by integrating new assessment criteria, analysing the dynamics of indicators over time, and adapting the model for use in various regional and social contexts.

References

- [1] Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences*, 12(5), 2589. <https://doi.org/10.3390/app12052589>
- [2] Alqarni, A. (2025). The relationship between cybersecurity awareness and data protection behaviors among Saudi secondary school students: The mediating role of cyber threat perception and the moderating role of internet usage duration. *Humanities and Social Sciences Communications*, 12(1), 1837. <https://doi.org/10.1057/s41599-025-06122-x>
- [3] Argyridou, E., Nifakos, S., Laoudias, C., Panda, S., Panaousis, E., Chandramouli, K., Navarro-Llobet, D., Mora Zamorano, J., Papachristou, P., & Bonacina, S. (2023). Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations: Concept Study. *Journal of Medical Internet Research*, 25, e41294. <https://doi.org/10.2196/41294>
- [4] Baraković, S., & Baraković Husić, J. (2023). Cyber hygiene knowledge, awareness, and behavioral practices of university students. *Information Security Journal: A Global Perspective*, 32(5), 347–370. <https://doi.org/10.1080/19393555.2022.2088428>
- [5] 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>
- [6] ENISA – European Union Agency for Cybersecurity. (2021). *Cybersecurity skills development in the EU*. <https://www.enisa.europa.eu/topics/cybersecurity-education>
- [7] European Commission. (2020). *European Skills Agenda for Sustainable Competitiveness, Social Fairness and Resilience*. Retrieved <https://ec.europa.eu/social/main.jsp?catId=1223>
- [8] European Commission. (2020). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's digital future (COM(2020) 67 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020DC0067>
- [9] European Commission, & High Representative of the Union for Foreign Affairs and Security Policy. (2021). *The EU's cybersecurity strategy for the digital decade* (JOIN(2020) 18 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52020JC0018>
- [10] European Union. (2022). Decision (EU) 2022/2481 of the European Parliament and of the Council establishing the Digital Decade Policy Programme 2030. *Official Journal of the European Union*, L 323. <https://eur-lex.europa.eu/eli/dec/2022/2481/oj/eng>
- [11] Polishchuk, I., Petrushko, I., Sehlanyk, 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>
- [12] Polishchuk, I., & Sehlanyk, V. (2026). Data from 315 respondents to assess the level of literacy of the population of different social profiles in the field of digital security (Ukraine) [Data set]. Zenodo. <https://doi.org/10.5281/ZENODO.18491825>
- [13] Prümmer, J., Van Steen, T., & Van Den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, 136, 103585. <https://doi.org/10.1016/j.cose.2023.103585>
- [14] Prümmer, J., Van Steen, T., & Van Den Berg, B. (2025). Assessing the effect of cybersecurity training on End-users: A Meta-analysis. *Computers & Security*, 150, 104206. <https://doi.org/10.1016/j.cose.2024.104206>
- [15] Rizal, M. A., & Setiawan, B. (2024). Information Security Awareness Literature Review: Focus Area for Measurement Instruments. *Procedia Computer Science*, 234, 1420–1427. <https://doi.org/10.1016/j.procs.2024.03.141>
- [16] 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), e14234. <https://doi.org/10.1016/j.heliyon.2023.e14234>
- [17] Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: A comparison between smartphones and computers. *Education and Information Technologies*, 26(2), 1721–1736. <https://doi.org/10.1007/s10639-020-10330-0>
- [18] United Nations. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development*. <https://sdgs.un.org/2030agenda>
- [19] United Nations Development Programme. (2025). *Sustainable development goals*. <https://www.undp.org/sustainable-development-goals>

Prof., D.Sc. Volodymyr Polishchuk
e-mail: volodymyr.polishchuk@tuke.sk
e-mail: volodymyr.polishchuk@uzhnu.edu.ua

He is a professor in the Department of Software Systems, Uzhhorod National University (Ukraine), and in the Department of Flight Training, Technical University of Košice (Slovakia). His research focuses on information technology, aviation, fuzzy logic, neuro-fuzzy networks, hybrid decision-support models, and complex systems under uncertainty and risk.

<https://orcid.org/0000-0003-4586-1333>



M.Sc. Vasyl Sehlanyk
e-mail: vasyi.sehlanyk@uzhnu.edu.ua

He is a Ph.D. student in the Department of Software Systems at Uzhhorod National University (Ukraine). He specializes in research and development in information systems and technologies, assessment of citizens' digital security levels, and software tool development.

<https://orcid.org/0009-0005-9958-3713>



Ph.D. Inna Polishchuk
e-mail: inna.polishchuk@tuke.sk
e-mail: inna.polishchuk@uzhnu.edu.ua

She is a senior lecturer in the Department of Software Systems at Uzhhorod National University (Ukraine) and a Ph.D. student in the Department of Flight Training at the Technical University of Košice (Slovakia). She specializes in research and development in the fields of information systems and technologies in tourism; decision support models and methods; information security.

<https://orcid.org/0009-0002-6395-4744>



M.Sc. Andrii Shafar
e-mail: andrii.shafar@uzhnu.edu.ua

He is a Ph.D. student in the Department of Software Systems at Uzhhorod National University (Ukraine). He specializes in research and development in information systems and technologies, digital transformation of the tourism industry, and software tool development.

<https://orcid.org/0009-0004-2445-8232>

