Journal homepage: https://itce.vn.ua/en

Information Technologies and Computer Engineering **Vol. 23, No. 2. 2026**

Article's History: Received: 21.12.2025 Revised: 01.05.2026
Accepted: 25.06.2026 Published: 03.08.2026

ISSN 1999-9941; e-ISSN 2078-6387
UDC 004.056:004.89
DOI: 10.31649/vitce/2.2026.78

A fuzzy model for assessing the behavioral component of digital security among different socio-demographic population groups

Volodymyr Polishchuk*
Doctor of Technical Sciences, Professor
Technical University of Kosice
04121, 7 Rampova Str., Kosice, Slovak Republic
Uzhhorod National University
88000, 3 Narodna Sq., Uzhhorod, Ukraine
https://orcid.org/0000-0003-4586-1333

Vasyl Sehlianyk
Postgraduate Student
Uzhhorod National University
88000, 3 Narodna Sq., Uzhhorod, Ukraine
https://orcid.org/0009-0005-9958-3713

Abstract. The relevance of the study was determined by the growing number of cyber threats in the digital environment and the need to develop methods for assessing the behavioural component of digital security, considering differences in digital literacy and technology use experience across various socio-demographic groups. The purpose of the study was to substantiate an approach to assessing the level of safe user behaviour in the digital environment based on socio-demographic differences in the population. To achieve this goal, methods of intelligent knowledge analysis, fuzzy set theory, multidimensional membership functions, and sociological data analysis were applied. The study developed an information model for assessing the behavioural component of digital security among the population based on a system of criteria that described users' safe interaction with the digital environment. Groups of indicators were formed to reflect citizens' awareness of cyber threats, their practices in using personal data protection tools, and their behavioural characteristics when interacting with digital resources. A fuzzy approach to determining the integral level of digital security based on multidimensional membership functions was proposed, which enables the integration of quantitative and qualitative assessment indicators and provides both numerical and linguistic evaluations of users' safe behaviour levels. The model was verified using questionnaire survey data obtained from 315 respondents representing different socio-demographic groups. The practical significance of the results obtained lies in the possibility of integrating the developed model into decision-support systems intended for monitoring the level of digital security of the population, segmenting socio-demographic groups by cyber-risk level, and substantiating targeted managerial, educational, and preventive measures aimed at improving digital literacy and users' safe behaviour

Keywords: cyber threats; safe digital behaviour; fuzzy logic; digital literacy; multicriteria assessment; membership functions; decision support

Introduction

The relevance of the study is determined by the growth of cyber threats in the digital environment and by the fact that users' vulnerability increasingly depends on their ability to recognise risks, protect personal data, and follow safe online practices. Since these behavioural patterns differ across socio-demographic groups because of unequal digital literacy and experience with technology, there is a need for analytical methods that enable differentiated assessment of the behavioural component of digital security. N.F. Khan *et al*. (2022) emphasised that the effectiveness

Suggested Citation:
Polishchuk, V., & Sehlianyk, V. (2026). A fuzzy model for assessing the behavioral component of digital security among different socio-demographic population groups. *Information Technologies and Computer Engineering*, 23(2), 78-89. doi: 10.31649/vitce/2.2026.78.

*Corresponding author (*volodymyr.polishchuk@tuke.sk*)

of countering cyber threats depends not only on technical means of information system protection, but also on users' awareness, behavioural practices, and willingness to follow the basic principles of cybersecurity. L. Bognár & L. Bottyán (2024) defined the behavioural component of digital security as a set of practical actions performed by users in the digital environment, including the use of strong passwords, multi-factor authentication, control over access to personal data, caution when opening electronic messages and links, and the ability to recognise potential cyber threats. In turn, R. Rohan *et al*. (2023) emphasised that behavioural factors often determine the actual level of user security in the digital space.

M. Zwilling *et al*. (2022) showed that cybersecurity awareness and behaviour may vary significantly depending on users' social profiles, professional environments, experience with digital technologies, and educational level. These findings support the view that different socio-demographic groups of the population demonstrate different levels of vulnerability to digital threats and therefore require a differentiated approach to the assessment and improvement of digital security. Furthermore, J. Prümmer *et al*. (2024) noted that a considerable part of contemporary research is focused on cybersecurity awareness, user training, and behaviour change methods, whereas the issue of formalised assessment of the behavioural component of digital security across different socio-demographic groups remains insufficiently developed. In turn, N.F. Khan *et al*. (2022) emphasised that most existing approaches rely on statistical analysis, questionnaire scales, or general behavioural classifications and do not always adequately account for uncertainty, the subjectivity of respondents' assessments, and the multi-criteria nature of the process under study. In this context, A. Almansoori *et al*. (2023) and K. Khadka & A.B. Ullah (2025) highlighted the potential of analytical approaches capable of integrating heterogeneous indicators and supporting the formalisation of complex human-cantered cybersecurity phenomena, which confirms the relevance of applying fuzzy modelling in this field. Thus, the problem of assessing the behavioural component of digital security among different socio-demographic groups is relevant both scientifically and practically. Its solution enables identification of the most vulnerable population groups, assessment of the level of development of safe behaviour in the digital environment, and formulation of recommendations to increase citizens' digital literacy and information security.

Despite the significant body of research on cybersecurity awareness and user behaviour, existing studies rarely provide formalised analytical models that simultaneously consider socio-demographic differences, multi-criteria behavioural indicators, and uncertainty inherent in survey-based assessments. This creates a methodological gap in the development of analytical tools for evaluating the behavioural component of digital security across population groups. The purpose of the study was to develop and validate a scientific and methodological approach to assessing safe behavioural practices in the digital environment across different socio-demographic groups of the population based on multidimensional membership functions and intelligent knowledge analysis methods. The scientific originality of the study lies in the development of a fuzzy model comprising an information model for assessing the behavioural component of citizens' digital security, a fuzzy approach to determining the aggregated level of digital security for individual respondents, and a method for the integral assessment of this indicator across various socio-demographic groups of the population.

Literature Review

In contemporary scientific literature, the behavioural aspects of digital security are regarded as a key dimension of the human factor in cybersecurity. Researchers emphasised that users' behaviour in the digital environment is shaped not only by technical knowledge, but also by psychological, educational, organisational, and social factors. This makes the study of cybersecurity behaviour an interdisciplinary field. A. Almansoori *et al*. (2023) summarised the main theoretical approaches to cybersecurity behaviour and showed that this phenomenon is multidimensional and cannot be fully explained within a single framework. R. Rohan *et al*. (2023) systematised the scales used to assess information security awareness and concluded that the lack of standardisation limits the comparability of empirical results. K. Khadka & A.B. Ullah (2025) further argued that human factors in cybersecurity should be analysed through the interaction of behavioural, organisational, and technological components.

A significant body of research also addresses cybersecurity awareness and user training. S. Chaudhary *et al*. (2023) identified important research gaps in awareness studies, especially for small and medium-sized enterprises, and noted that awareness programs do not always lead to measurable behavioural change. Effective cybersecurity training increasingly relies on interactive and adaptive approaches tailored to users' real digital practices. In turn, T. van Steen & J.R.A. Deeleman (2021) demonstrated that gamification can improve user engagement and support the development of safer digital behaviour. Some studies focused on behavioural change and its measurement tools. D. Kovalchuk (2025) substantiated the feasibility of using large language models for automated real-time analysis of cyber threats and emphasised their potential for rapid detection, interpretation, and decision support in cybersecurity. S. Bender *et al*. (2024) demonstrated the effectiveness of just-in-time interventions for improving online safety, while L. Bognár & L. Bottyán (2024) developed and validated a scale of personal cybersecurity awareness among university students.

A significant part of contemporary research aimed to identify differences in digital security across user groups. M. Zwilling *et al*. (2022) empirically confirmed the relationship among awareness, knowledge, and actual cybersecurity behaviour. C.S. Lee & D. Kim (2023) analysed the

development of protective cyber behaviour in the context of South Korea, emphasising the role of socio-cultural factors. Their study showed that users' intention to engage in secure behaviour is significantly influenced by both cognitive factors (such as knowledge and awareness) and behavioural determinants. Similarly, D. Branley-Bell *et al*. (2022) examined cybersecurity behaviour in relation to demographic characteristics and gender groups. Their findings indicated that younger users tend to demonstrate higher technical confidence but are more prone to risky online behaviour, whereas older users exhibit more cautious patterns. Gender differences were also observed, particularly in risk perception and adoption of protective measures, suggesting that cybersecurity strategies should be tailored to specific demographic profiles rather than applied uniformly.

The behavioural component of digital security was also actively studied in relation to age characteristics. M. Alanazi *et al*. (2022) identified factors influencing the cybersecurity behaviour of young people. Further, B. Morrison *et al*. (2021) showed that older users often demonstrated greater caution but lower confidence in their own digital protective practices. These findings confirmed the feasibility of a differentiated approach to assessing the behavioural component of digital security across different socio-demographic groups. A substantial body of research addressed phishing and social engineering as areas in which the human factor played a decisive role. G. Desolda *et al*. (2021), in a systematic review, demonstrated that the effectiveness of phishing attacks largely depended on users' cognitive and behavioural characteristics. E. Morrow (2024) analysed the content and trends of phishing messages in higher education, while Y. Hong & S. Furnell (2021) argued that cyber habits were shaped not only by knowledge, but also by situational support and the context of digital technology use.

Applied studies in specific sectors also made an important contribution. E. Argyridou *et al*. (2023) proposed a cyber hygiene methodology aimed at increasing cyber awareness and improving data protection in healthcare organisations. K. Hasegawa *et al*. (2024) analysed cybersecurity interventions in healthcare organisations in low- and middle-income countries. Separate studies also attempted to formalise indicators and construct assessment models for digital security behaviour. B.H. Nguyen & H.N.Q. Le (2024) investigated information security awareness through the KAB model and showed that age and education significantly moderated the relationships among knowledge, attitudes, and behaviour. L. Bognár (2025) proposed an approach to predicting cyber incidents based on self-reported behavioural and psychological indicators, demonstrating the analytical value of combining subjective and behavioural variables in cybersecurity research. These studies confirmed the importance of formalised assessment tools, but they also showed that existing approaches were mainly oriented toward isolated indicators or linear relationships.

Taken together, the reviewed literature demonstrated that cybersecurity awareness, user training, phishing vulnerability, and behavioural determinants of digital security were sufficiently represented in contemporary research. However, approaches capable of simultaneously accounting for the multi-criteria structure of safe digital behaviour, socio-demographic differentiation of the population, and the vagueness of respondents' self-assessments remained insufficiently developed. This limitation was especially important because the behavioural component of digital security was formed at the intersection of quantitative and qualitative characteristics, many of which could not be described adequately by strict deterministic boundaries.

Materials and Methods

This study was based on the authors' previous research (Polishchuk & Sehlianyk, 2026). The methodological framework of the study included survey-based data collection, identification of behavioural cybersecurity indicators, normalisation of variables, construction of membership functions, fuzzy aggregation of criteria, and interpretation of the resulting linguistic levels. From March to June 2025, a questionnaire survey was conducted in the Zakarpattia Oblast, during which empirical data were collected from 315 respondents using a 49-item instrument included in the information assessment model. The survey sample was formed to represent the target population by covering respondents with diverse socio-demographic characteristics; 60% of the participants were men and 40% were women, 98.5% belonged to the working-age population and actively used digital technologies. The survey was anonymous, participation was voluntary, and the respondents provided informed consent to participate in the study and to the processing of their data. The collection and processing of personal data were organised in accordance with the ethical principles of voluntariness, confidentiality, and data protection reflected in the European Commission (2021) guidance on ethics and data protection in research. The collected data were used to verify the proposed fuzzy model and to perform quantitative and linguistic interpretation of the obtained results.

A certain region R and the citizens $C = \{c_1; c_2;...; c_n\}$ belonging to this region were considered. Each citizen was characterised by a set of socio-demographic characteristics, forming the set $S = \{s_1, s_2,..., s_m\}$. Combinations of these characteristics formed the set of socio-demographic groups of the population $ST = \{ST_1, ST_2,...,ST_k\}$. Citizens were given a questionnaire with a set of text questions K (assessment criteria), which were grouped into G to determine the level of behavioural digital security. The answers received, together with the data processing system, represented an information model for assessing the level of behavioural digital security of citizens – K_{DS}. A fuzzy model for evaluating this component across socio-demographic groups was proposed in the form of an operator:

$$M_4 (R, C, ST, K_{DS}) | Y(f_4). \quad (1)$$

The operator M_4 based on the input data R, C, ST, K_{DS} matched the output value $Y(f_4) = \{\vartheta_{DS} (c); y_{DS}; DS\}$, which

consisted of the following quantities: $\vartheta_{DS}(c)$ – aggregated assessment of the level of behavioural digital security in terms of a citizen; y_{DS} – integral indicator of the level of the behavioural component of digital security of the population of different socio-demographic groups; *DS* – recommendations for increasing the level of behavioural digital security of the population of different socio-demographic groups. Figure 1 presents a structural diagram of a fuzzy model.

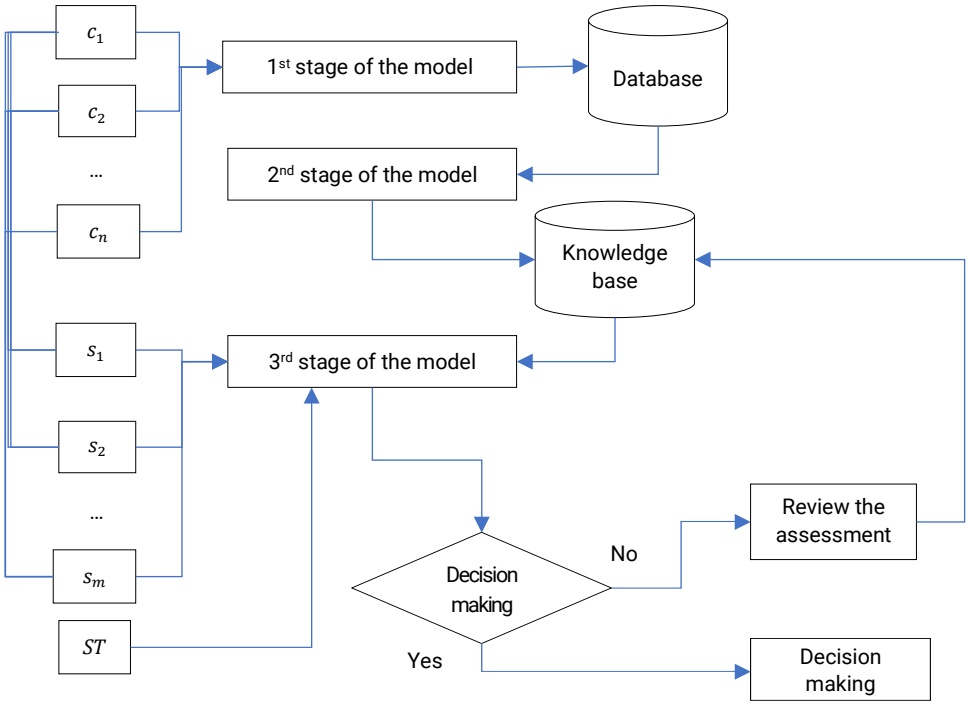

Figure 1. Structural diagram of a fuzzy model

Source: completed by the authors

The diagram shows the main stages of information processing, from the generation of input data to the obtaining of an integrated assessment and its linguistic interpretation. The model's input parameters consisted of the study region , the set of citizens , the socio-demographic characteristics *S*, the socio-demographic groups *ST* formed based on , and the information assessment model , which contained the criteria for assessing the behavioural component of digital security. At the first stage, an information model was generated based on a questionnaire survey, aggregation of the obtained score estimates by groups of criteria, and their fuzzification using membership functions. As a result, fuzzy estimates of each citizen's level of digital security practices were determined. The results represented the research database. The second stage involved aggregating the obtained fuzzy estimates considering the weight coefficients for the groups of criteria. For this, different types of convolutions were used, which enabled an aggregated estimate of the level of behavioural digital security for an individual citizen. The obtained results were recorded in the knowledge base. At the third stage, the aggregation results were integrated with respondents' socio-demographic characteristics. This allowed determining an integral indicator of the behavioural component of digital security for different socio-demographic groups and interpreting it linguistically. The fuzzy model was presented in three stages. The first stage presented an information model (K_{DS}) for assessing citizens' behavioural digital security based on criteria grouped into three categories. Evaluation was performed on a 1-10 scale, where 1 indicated a minimal and 10 – a maximal level of knowledge.

G_1 – safe use of digital services.

K_{11} – frequency of changing passwords for personal accounts.

K_{12} – use of complex passwords.

K_{13} – use of two-factor authentication.

K_{14} – use of device protection tools.

G_2 – protection of personal data and confidentiality.

K_{21} – caution when entering personal data on websites.

K_{22} – control access to personal data in social networks.

K_{23} – caution about sharing personal information on social networks.

K_{24} – use of different passwords for different digital services.

G_3 – protection of personal data and confidentiality.

K_{31} – ability to recognise phishing messages and fraudulent activities.

K_{32} – ability to determine the safety of websites.

K_{33} – ability to respond to cyber incidents.

K_{34} – ability to verify information and avoid manipulation.

After the survey, scores were obtained, which were designated O_{11}, O_{12},..., O_{34} respectively, according to the criteria K_{11}, K_{12},..., K_{34}. First, one overall score was obtained within the group of criteria:

$$\lambda_g(c_i) = \sum_{p=1}^{l} O_{gp}(c_i), \quad (2)$$

where l – number of criteria in the group G_g ($g = \{1; 2; 3\}$), i – respondent number, $i = \overline{1,n}$.

Fuzzification of input data was carried out based on the methods of knowledge mining using the S-shaped membership function (Skare *et al.*, 2026). After evaluation, the scores $\lambda_g(c_i)$ were obtained. For their fuzzification, it was proposed to use intellectual knowledge analysis and an S-shaped membership function:

$$\mu_g(c_i) = \begin{cases} 0, & \lambda_g(c_i) \le 0; \\ \frac{(\lambda_g(c_i))^2}{800}, & 0 < \lambda_g(c_i) \le 20; \\ 1 - \frac{(40-\lambda_g(c_i))^2}{800}, & 20 < \lambda_g(c_i) < 40; \\ 1, & \lambda_g(c_i) \ge 40. \end{cases} \quad i = \overline{1,n}. \quad (3)$$

The value $\mu_g(c_i) \to 1$ indicated a high level of development of behavioural practices of digital security in the corresponding group of criteria, while $\mu_g(c_i) \to 0$ characterised a low level of their development. Thus, at the end of the first stage, the assessments were aggregated within each criterion group to obtain a generalised indicator $\lambda_g(c_i)$. To account for the assessment's uncertainty, the obtained values were fuzzified, allowing determination of the degree of belonging of $\mu_g(c_i)$ to the corresponding level of the behavioural component of digital security.

At the second stage of the model, $\vartheta_{DS}(c_i)$ was derived – an aggregated assessment of the level of behavioural digital security in terms of a citizen. First, the importance of the groups of criteria was considered. The decision maker (DM) set the weights for each group $\{\alpha_1, \alpha_2, \alpha_3\}$ from some interval [1; 10]:

$$\beta_g = \frac{\alpha_g}{\sum_{g=1}^{3} \alpha_g}, \beta_g \in [0; 1]. \quad (4)$$

Next, one of the convolutions was used separately by citizen ($i = \overline{1,n}$):

$$\vartheta_{DS1}(c_i) = \frac{1}{\sum_{g=1}^{3} \frac{\beta_g}{\mu_g(c_i)}}; \quad (5)$$

$$\vartheta_{DS2}(c_i) = \prod_{g=1}^{3} \left(\mu_g(c_i)\right)^{\beta_g}; \quad (6)$$

$$\vartheta_{DS3}(c_i) = \sum_{g=1}^{3} \beta_g \cdot \mu_g(c_i); \quad (7)$$

$$\vartheta_{DS4}(c_i) = \sqrt{\sum_{g=1}^{3} \beta_g \cdot \left(\mu_g(c_i)\right)^2}. \quad (8)$$

Thus, aggregated estimates of behavioural digital security for a citizen were obtained. The choice of the type of convolution determined the DM, and the resulting aggregated estimate $\vartheta_{DS}(c_i) \in [0;1]$. Moreover, when $\vartheta_{DS1}(c_i) \to 1$, then this determined a high level of development of the behavioural component of digital security of a citizen, which indicates the proper use of safe practices in the digital environment, effective protection of personal data, and the ability to recognise and counteract cyber threats timely.

Here, the integral indicator y_{DS} was determined, and *DS*, recommendations were formulated, reflecting the level of awareness among socio-demographic groups in the population regarding the behavioural component of digital security. First, for each citizen, it was necessary to consider their socio-demographic characteristics $S = \{s_1; s_2; \ldots; s_m\}$, with formalised answers. The following are the most common ones proposed. Gender – σ_1. The linguistic evaluation was as follows: s_1 = "man"; s_2 = "woman". Age – σ_2. For this demographic assessment, the values of unified intervals regarding the number of years of citizens were accepted: s_3 = "if from 18 to 25"; s_4 = "if from 26 to 42"; s_5 = "if from 43 to 55"; s_6 = "if from 56 to 65"; s_7 = "if over 65". Primary socio-economic status – . For this demographic characteristic, the following indicators were considered: s_8 = "Student"; s_9 = "Employed"; s_{10} = "Unemployed"; s_{11} = "Pregnancy/guardianship"; s_{12} = "Pensioner". Education – σ_4. For this demographic characteristic, the highest completed education was considered: s_{13} = "Complete general secondary education"; s_{14} = "Vocational and technical education"; s_{15} = "Higher education level 1 (Bachelor)"; s_{16} = "Higher education level 2 (Master)"; s_{17}= "Higher education level 3 (PhD) or higher". Average net monthly income – σ_5. For quantitative consideration, the following formalisation was carried out: s_{18} = "up to UAH 10,000"; s_{19}= "UAH 10,000-14,000"; s_{20} = "UAH 14,000-18,000"; s_{21} = "UAH 18,000-22,000"; s_{22} = "UAH 22,000-30,000"; s_{23} = "more than UAH 30,000". Marital status – σ_6. For this socio-demographic characteristic, the following formalisation was carried out: s_{24} = "single"; s_{25} = "married"; s_{26} = "divorced"; s_{27} = "widowed". Next, the arithmetic mean of the obtained aggregated estimates of the level of behavioural digital security in terms of socio-demographic characteristics was calculated:

$$\psi_{DS}(s_j) = \frac{1}{r_j} \sum_{q=1}^{r_j} \vartheta_{DS}(c_q), \quad (9)$$

where s_j – socio-demographic characteristic, $j = \overline{1,m}$; r_j – number of citizens related to the characteristic s_j.

Equal weighting was assumed, as no prior empirical evidence or theoretical substantiation exists to assign different importance to specific socio-demographic factors; therefore, all factors were treated as equally significant to avoid introducing subjective bias. Next, the integral indicator of the behavioural component of digital security for different socio-demographic groups (y_{DS}) was derived. Groups were formed by grouping characteristics S according to some rule T. The DM determined this rule for including various socio-demographic characteristics. For example, a combination of the proposed demographic characteristics was proposed. Thus, one value from the set was obtained, which was denoted as follows: $\sigma_1^* = \{s_1; s_2\}$; $\sigma_2^* = \{s_3; s_4; \ldots; s_7\}$; $\sigma_3^* = \{s_8; s_{11}; \ldots; s_{12}\}$; $\sigma_4^* = \{s_{12}; s_{13}; \ldots; s_{17}\}$; $\sigma_5^* = \{s_{18}; s_{19}; \ldots; s_{23}\}$; $\sigma_6^* = \{s_{24}; s_{25}; \ldots; s_{27}\}$. The integral assessment was obtained using multidimensional membership functions. In six-dimensional space, uncertainty was modelled using conical or pyramidal membership functions:

$$y_{DS(C)} = \begin{cases} 1-\Delta, \text{if } \Delta < 1, \\ 0, \text{otherwise.} \end{cases} \quad (10)$$

where $\Delta = \frac{1}{6} \cdot \sqrt{(\psi_{DS}(\sigma_1^*)-1)^2 + (\psi_{DS}(\sigma_2^*)-1)^2 + \cdots + (\psi_{DS}(\sigma_6^*)-1)^2}$.

The pyramidal membership function will have the form:

$$y_{DS(P)} = max\left\{\left(1 - \frac{1}{6}(|\psi_{DS}(\sigma_1^*)-1| + |\psi_{DS}(\sigma_2^*) - \right.\right.$$
$$\left.\left. - 1| + \cdots + |\psi_{DS}(\sigma_6^*)-1|)\right); 0\right\}. \quad (11)$$

Conical and pyramidal membership functions were selected due to their ability to represent gradual changes in membership values and provided interpretable aggregation in a multidimensional space. The conical function ensured smoother transitions, whereas the pyramidal function provided more linear and clearly bounded changes. The type of membership function was selected by the systems analyst based on the desired shape of membership decline in the multidimensional space and the interpretability requirements of the assessment procedure. The conical function was appropriate for smoother transitions, whereas the pyramidal function was preferable for linear and more clearly bounded changes in membership values. At the final stage, the integral estimates $y_{DS(C)}$ or $y_{DS(P)}$ were interpreted using a five-level linguistic scale describing the degree of behavioural digital security. The threshold values between the linguistic levels were determined either based on expert calibration, empirical distribution of the data, or additional validation procedures, which were considered a separate stage of model tuning. Depending on the obtained value of the integral indicator y_{DS}, the following recommendations were formed:

- $y_{DS} \in [0.8; 1]$ – ds_1 "high level". It is recommended to maintain the existing level of digital security, periodically update knowledge about new cyber threats, and spread practices of safe behaviour in the digital environment.
- $y_{DS} \in [0.7; 0.8]$ – ds_2 "above average level". It is advisable to raise awareness of advanced methods of protecting personal data, use multi-factor authentication, and regularly update cyber protection tools.
- $y_{DS} \in [0.6; 0.7]$ – ds_3 "intermediate level". It is recommended to undergo thematic training or educational programmes on digital security, and develop skills in recognising cyber threats and using online services safely.
- $y_{DS} \in [0.5; 0.6]$ – ds_4 "low level". It is necessary to purposefully increase the level of digital literacy, familiarise users with the basic rules of personal data protection and safe behaviour on the Internet.
- $y_{DS} \in [0;0.5]$ – ds_5 "very low level". It is recommended to undergo systematic training in digital security fundamentals, including basic principles of cyber hygiene, account protection, and cyber threat recognition.

The distinction between levels was determined by the systems analyst based on the empirical distribution of the obtained integral estimates, considering their concentration, boundary values, and separation between adjacent groups. The applied approach helped to align the linguistic levels with the actual structure of the empirical data and to ensure a more substantiated interpretation of the assessment results.

Results

The proposed fuzzy model was verified using the full dataset obtained from a questionnaire survey of 315 respondents. At this stage, the purpose was to examine how the initial empirical assessments of respondents were distributed across the selected criteria groups and to determine whether the input data were suitable for subsequent fuzzy transformation and integral assessment. Table 1 presents fragments of the initial survey data included in the information model K_{DS}. Here, c_1, c_2, c_3,..., c_{315} denote individual respondents, while the numerical values represent their scores for the corresponding criteria on the adopted assessment scale.

Table 1. Input data fragments

Criteria groups	Criteria	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	8	3	...	2
	K_{14}	8	9	7	...	8
G_2	K_{21}	6	9	7	...	8
	K_{22}	7	9	6	...	6
	K_{23}	7	8	7	...	8
	K_{24}	7	6	6	...	6
G_3	K_{31}	8	9	4	...	6
	K_{32}	7	9	8	...	7
	K_{33}	7	8	8	...	6
	K_{34}	7	8	7	...	8

Note: G_1 – safe use of digital services; K_{11} – frequency of changing passwords for personal accounts; K_{12} – use of complex passwords; K_{13} – use of two-factor authentication; K14 – use of device protection tools; G_2 – protection of personal data and confidentiality; K_{21} – caution when entering personal data on websites; K_{22} – control of access to personal data in social networks; K_{23} – caution about sharing personal information on social networks; K_{24} – use of different passwords for different digital services; G_3 – protection of personal data and confidentiality; K_{31} –ability to recognise phishing messages and fraudulent activities; K_{32} – ability to determine the safety of websites; K_{33} – ability to respond to cyber incidents; K_{34} – ability to verify information and avoid manipulation
Source: compiled by the authors

The data presented in Table 1 showed that the respondents' scores were generally concentrated in the medium-to-high range, indicating a moderate or sufficient level of development of the behavioural component of digital security for a considerable part of the sample. Furthermore, noticeable variation across individual criteria and respondents pointed to the heterogeneity of behavioural practices in the digital environment. A comparison of groups G_1, G_2, and G_3 suggested that relatively higher and more stable scores were more frequently observed in G_2 and partly in G_3, whereas G_1 demonstrated greater variability, which may indicate differences in the development of specific components of safe digital behaviour. To assess the analytical suitability of the obtained scores for fuzzy interpretation, the initial values were aggregated within each criteria group and then transformed into fuzzy estimates. This stage helped to pass from raw questionnaire scores to normalised values reflecting the degree of membership of each respondent's result to the corresponding level of behavioural digital security. Table 2 presents fragments of the aggregated values λ_g and their corresponding fuzzified estimates μ_g for the three criteria groups. These results were used to identify the extent to which the respondents' primary assessments retained inter-group differences after fuzzy transformation and to provide the basis for the next stage of integral aggregation.

Table 2. Results of fuzzified input data fragments

Criteria groups	Value	c_1	c_2	c_3	...	c_{315}
G_1	λ_1	28	30	26	...	19
	μ_1	0.82	0.875	0.755	...	0.451
G_2	λ_2	27	32	26	...	28
	μ_2	0.789	0.92	0.755	...	0.82
G_3	λ_3	29	34	27	...	27
	μ_3	0.849	0.955	0.789	...	0.789

Source: compiled by the authors

The results shown in Table 2 indicated that the fuzzification procedure preserved the general structure of the empirical data while transforming the initial scores into analytically comparable membership values. The aggregated values λ_g remained in the medium-to-high range for most respondents, and the corresponding membership values μ_g were also predominantly above 0.7, which indicated a generally sufficient level of development of the behavioural component of digital security in the sample. However, lower fuzzified values were also observed for some respondents, reflecting weaker development of safe digital behaviour in particular criteria groups.

After fuzzification, the initial raw scores were converted into normalised membership values that expressed the degree to which each respondent's result corresponded to the selected level of digital security behaviour. This transformation did not distort the empirical data, since the relative differences between respondents and between criteria groups remained visible after conversion. On the contrary, fuzzification made the data more suitable for further aggregation and comparison by reducing scale heterogeneity while preserving the original variation structure of the survey results. For example, respondent c_2 demonstrated consistently high values across all three groups, while respondent c_3 had noticeably lower values in some components, especially in G_1, which pointed to uneven development of safe digital behaviour across criteria groups. Thus, Table 2 confirmed that fuzzy transformation not only standardised the data but also preserved the variability necessary for subsequent integral evaluation.

At the next stage, the fuzzified values were combined into aggregated estimates of the behavioural component of digital security for each respondent. Considering the selected weight coefficients for the three criteria groups ($\alpha_1 = 9$, $\alpha_2 = 10$, $\alpha_3 = 8$), their normalised values were $\beta_1 = 0.33$, $\beta_2 = 0.37$, and $\beta_3 = 0.30$, which indicated a slightly greater contribution of group G_2 to the final result. The resulting aggregated estimates showed noticeable differences across respondents. For example, the values $\vartheta_{DS3}(c_1) = 0.817$, $\vartheta_{DS3}(c_2) = 0.916$, $\vartheta_{DS3}(c_3) = 0.765$, and $\vartheta_{DS3}(c_{315}) = 0.689$ reflected different degrees of development of safe digital behaviour. Respondent c_2 demonstrated a consistently high aggregated result, whereas respondent c_{315} showed a lower value, indicating weaker behavioural readiness in the digital environment. To interpret the obtained aggregated estimates in relation to population structure, the respondent-level results were further linked to socio-demographic characteristics. Table 3 presents fragments of the socio-demographic data used for this stage of analysis. These variables allowed moving from individual-level fuzzy estimates to the integral assessment of selected socio-demographic profiles.

Table 3. Fragments of socio-demographic data

Characteristics	c_1	c_2	c_3	...	c_{315}
σ_1	Man	Woman	Man	...	Man
σ_2	39	20	21	...	24
σ_3	Employed	Student	Student	...	Student

Table 3. Continued

Characteristics	c_1	c_2	c_3	...	c_{315}
σ_4	Higher education level 2 (PhD) or higher	Higher education level 1 (bachelor's degree)	Completed general secondary education	...	Vocational and technical education
σ_5	UAH 14,000-18,000	up to UAH 10,000	up to UAH 10,000	...	UAH 10,000-14,000
σ_6	married	single / unmarried	single / unmarried	...	married

Note: σ_1 – sex; σ_2 – age; σ_3 – primary socio-economic status; σ_4 – education; σ_5 – average net monthly income; σ_6 – marital status
Source: compiled by the authors

The socio-demographic data shown in Table 3 confirmed that the sample included respondents with different social profiles, which created the basis for differentiated group-level assessment. The table demonstrated the representation of groups by gender, age, socio-economic status, education level, income, and marital status, thus covering the main characteristics required for profile-based interpretation of digital security behaviour. The data suggested the presence of some dominant categories, in particular, students and respondents of younger age groups, which was consistent with the structure of the surveyed population. The sample also showed clear variability across age, educational background, and income levels. Respondents ranged from young adults to middle-aged individuals, represented different levels of completed education, and belonged to several income categories. Such diversity was important for the model because it allowed the integral estimates to be interpreted not for a homogeneous population, but for socio-demographic groups with different levels of social and digital experience. In this way, Table 3 served not merely as a descriptive supplement, but as the empirical basis for constructing and interpreting integral estimates for selected respondent groups.

For the group-level interpretation of results, an illustrative socio-demographic profile was selected: female, aged 18-25, student, bachelor-level education, income up to UAH 10,000, and single marital status. For this profile, the partial averaged values were $\psi_{DS}(s_2) = 0.70$, $\psi_{DS}(s_3) = 0.76$, $\psi_{DS}(s_8) = 0.77$, $\psi_{DS}(s_{15}) = 0.72$, $\psi_{DS}(s_{18}) = 0.77$, and $\psi_{DS}(s_{24}) = 0.76$. These values indicated a relatively consistent distribution of medium-to-high assessments across the selected socio-demographic dimensions. As an illustrative example of applying the proposed model to one selected socio-demographic group, the conical membership function was used, resulting in the integral estimate $y_{DS(C)} = 0.896$. According to the adopted interpretive scale, this value corresponded to the "high level" category. This result indicated that the considered socio-demographic group demonstrated a sufficiently formed behavioural component of digital security, including adherence to cyber hygiene practices, more careful interaction with digital services, and a higher ability to recognise potential cyber threats.

The application of the proposed fuzzy model to the full dataset helped to obtain aggregated respondent-level estimates and to transform them into integral assessments for selected socio-demographic groups. The calculated respondent-level values ranged from 0.02 to 1, while the mean aggregated estimate for the full sample was 0.7583. These results indicated that the behavioural component of digital security in the studied population was generally formed at a medium-to-high level. Furthermore, the wide spread of values pointed to substantial inter-respondent variation and confirmed that the sample was not homogeneous in terms of safe digital behaviour. The obtained results also showed that differences remained visible after fuzzification and aggregation, which confirmed that the model preserved the structure of the empirical data and provided a basis for differentiated group-level interpretation. Variation in the aggregated estimates reflected differences in awareness, protective practices, and interaction with digital services across respondents. This indicated that the proposed approach did not reduce the survey data to an overly generalised form but retained the variability necessary for subsequent comparison of socio-demographic profiles.

A comparison of socio-demographic groups showed that the integral estimates varied depending on the combination of gender, age, socio-economic status, education, income, and marital status. For example, the illustrative group analysed in this study demonstrated a high integral estimate ($y_{DS(C)} = 0.896$), which corresponded to a high level of development of the behavioural component of digital security. Such variation confirmed the possibility of using the model for differentiated assessment of population groups and for identifying both relatively better-formed and less-developed profiles of digital security behaviour within the overall sample. From the analytical standpoint, the results suggested that the proposed model was sensitive to both individual and group-level differences. This sensitivity was reflected in the fact that respondents with similar raw questionnaire scores retained close membership values after fuzzification, whereas respondents with less consistent behavioural profiles produced lower aggregated estimates. In this way, the fuzzy procedure supported a gradual rather than rigid interpretation of behavioural digital security, which was especially important for survey-based data with partly subjective and linguistically interpretable responses.

A preliminary indication of model stability was observed in the consistency of the obtained estimates across

the successive stages of transformation. The transition from raw scores to group aggregates, from aggregates to membership values, and from membership values to integral estimates did not eliminate the initial structure of differences in the data. Instead, it converted the survey results into a form suitable for multidimensional interpretation. Therefore, the present results should be interpreted as confirming the feasibility of applying the proposed model to empirical data rather than as a final proof of its universal robustness. Taken together, the results demonstrated that the proposed fuzzy model could be applied to the assessment of the behavioural component of digital security in socio-demographically differentiated populations. The possibility of converting heterogeneous survey responses into interpretable integral estimates that could support further analytical comparison of population groups was shown. Thus, the presented example of model testing confirmed the possibility of applying the proposed approach to the assessment of the behavioural component of digital security in selected socio-demographic groups. The obtained results also indicated the potential usefulness of the model for monitoring-related tasks and for supporting management decision-making aimed at improving citizens' digital literacy and information security.

Discussion

The obtained results should be interpreted in the context of recent studies that view digital security behaviour as a multidimensional phenomenon shaped by cognitive, behavioural, and social factors. In this respect, the present study was conceptually close to the paper by B. Hanus *et al*. (2018), who argued that security awareness should not be reduced to a single indicator, but should be treated as a multidimensional construct with several interacting components. The current results were consistent with this opinion, since the developed model also relied on several criteria groups rather than a single summary variable. Furthermore, unlike that study, the present paper did not focus on conceptual definition alone, but on the formal aggregation of these dimensions into an integral estimate for socio-demographic groups. A similar comparison may be drawn with the study by S.M. Kennison & E. Chan-Tin (2020), who showed that risky cybersecurity behaviour was predicted not only by cybersecurity knowledge, but also by personality traits and general risk-taking tendencies. Their findings confirmed the analytical value of self-reported behavioural data, which was also used in the present study as the empirical basis for modelling. However, whereas authors focused on predicting risky behaviour at the individual level, the current study addressed the integral assessment of the behavioural component of digital security across socio-demographic profiles.

The findings of the present study may also be compared with the results of K. Šolić *et al*. (2024), who used the Behavioural-Cognitive Internet Security Questionnaire to investigate information security awareness. Their research confirmed that survey-based instruments can capture several dimensions of digital security awareness and can be used to differentiate users by the level of their security-related behaviour and knowledge. This was similar to the current study, where the empirical basis also consisted of structured questionnaire responses reflecting several aspects of user behaviour. The difference lay in the methodological purpose: while K. Šolić *et al*. mainly relied on a validated measurement instrument to assess awareness, the present study proposed a fuzzy analytical procedure that transformed such data into aggregated and linguistically interpretable integral estimates.

Another important point of comparison concerned the relationship between awareness and action. P. Mayer *et al*. (2023) showed that even when individuals were aware of data breaches affecting them, this awareness did not always translate into sustained protective action. Their results highlighted the gap between perception, intention, and actual behavioural response. This observation is relevant to the present study because it supports the idea that digital security behaviour should be assessed through a combination of indicators rather than inferred from awareness alone. In the present study, this logic was reflected in the use of several criteria groups that jointly captured protective routines, data-related caution, and threat recognition practices.

The present results were also comparable with the study by T. Karayel *et al*. (2025), who examined cyber hygiene practices in remote work settings and found that organisational security measures were significantly associated with employees' cyber hygiene behaviour, with differences also observed between sectors. Their conclusions are important because they confirm that digital security behaviour is context-dependent and varies across user groups exposed to different social and organisational conditions. This was broadly consistent with the present study, where socio-demographic differentiation was treated as analytically significant and where the observed range of aggregated estimates, from 0.020 to 1.000, indicated substantial heterogeneity among respondents. Furthermore, the current study extended this perspective by embedding such heterogeneity into a fuzzy model that produced integral estimates for selected social profiles rather than only reporting correlational differences.

From a methodological perspective, the current results supported the appropriateness of using fuzzy logic for this class of problems. The surveyed population demonstrated a wide spread of aggregated respondent-level values, while the mean estimate for the full sample was 0.7583, indicating a generally medium-to-high level of the behavioural component of digital security with pronounced inter-respondent variation. Such a result suggested that the phenomenon under study could not be adequately represented by rigid binary categories. In this respect, the present study differed from approaches based solely on crisp classification or simple average

scoring, because the fuzzy procedure preserved gradual transitions between low, moderate, and high levels of digital security behaviour. This feature was especially important for self-reported behavioural data, where uncertainty and partial membership are methodologically more realistic than strict deterministic boundaries. The multidimensional conception of security awareness emphasised by B. Hanus *et al*. (2018) and the behavioural variability demonstrated by S.M. Kennison & E. Chan-Tin (2020) indirectly supported this methodological choice.

Thus, the comparison with the cited literature also made the limitations of the current study more visible. First, the model was verified on one regional dataset of 315 respondents, whereas several related studies relied on larger or separately validated survey settings. Second, one stage of the aggregation procedure treated socio-demographic characteristics as equally weighted, which simplified the model but could reduce sensitivity to the unequal influence of factors. Third, the linguistic interpretation thresholds were determined empirically rather than derived automatically from a complete fuzzy inference system, which means that the interpretive scale should be viewed as calibrated rather than universal. In this sense, the present study should be regarded as demonstrating the applicability of the proposed approach rather than providing a final standardised instrument. This interpretation is also consistent with P. Mayer *et al*. (2023), who showed that behavioural security phenomena often remain situationally dependent, and with T. Karayel *et al*. (2025), who pointed to contextual variation in cyber hygiene practices.

Overall, in comparison with recent related studies, the present research contributed primarily at the methodological level. It did not attempt to redefine the known determinants of digital security behaviour but offered a formalised way to integrate multidimensional questionnaire data, socio-demographic differentiation, and partial uncertainty into a single analytical framework. In that sense, the results were broadly consistent with the literature emphasising multidimensionality, behavioural variability, and the gap between awareness and practice, while the distinctive contribution of the current study lay in transforming these features into an interpretable fuzzy assessment procedure.

Conclusions

This study addressed the problem of assessing the behavioural component of digital security across different socio-demographic groups of the population. The research was aimed at developing and verifying a fuzzy approach that helped to transform questionnaire-based empirical data into integral estimates reflecting the level of safe digital behaviour in groups with different social profiles. An information model was constructed based on grouped criteria characterising safe use of digital services, personal data protection practices, and the ability to recognise cyber threats. On this basis, a fuzzy procedure was implemented that included aggregation of respondents' scores within criteria groups, fuzzification of the obtained values, and derivation of aggregated respondent-level estimates. These estimates were then used for the integral assessment of selected socio-demographic profiles through multidimensional membership functions.

The verification performed on empirical data from a questionnaire survey of 315 respondents showed that the aggregated respondent-level estimates ranged from 0.02 to 1, with a mean value of 0.7583. This indicated that the behavioural component of digital security in the studied sample was generally formed at a medium-to-high level, although considerable variation between respondents remained visible. The results also showed that the applied fuzzy procedure preserved inter-respondent differences after aggregation and fuzzification, which made differentiated group-level interpretation possible. For the illustrative socio-demographic profile considered in the study, the integral estimate was 0.896, corresponding to a high level of development of the behavioural component of digital security.

The obtained results showed that the behavioural component of digital security should be analysed as a multidimensional phenomenon that varies across socio-demographic groups and cannot be adequately represented by isolated indicators alone. The proposed approach helped to combine heterogeneous behavioural characteristics within a unified assessment framework and to obtain interpretable integral estimates for selected social profiles. The study had several limitations. The model was verified on one regional sample of 315 respondents, which limits the generalisability of the obtained results. In addition, the aggregation of socio-demographic characteristics was performed using equal weights, and the thresholds of linguistic interpretation were determined empirically for the present dataset. Further research should focus on validation of the model on independent datasets from other regions, broader comparison of socio-demographic groups, refinement of weighting procedures, and sensitivity analysis of membership functions and linguistic threshold settings.

Acknowledgements

None.

Funding

This research was conducted within the framework of the scientific projects for young researchers "Protection of Information Security in the Management of International Cooperation Projects Based on Ensuring the National Security of Ukraine" (DB-921M) and "Protection of Personal Data in the Context of the Development of Artificial Intelligence and the Internet of Things: Legal and Technical Aspects" (DB-924M), funded by the Ministry of Education and Science of Ukraine.

Conflict of Interest

None.

References

[1] Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, 136, article number 107376. doi: 10.1016/j.chb.2022.107376.

[2] 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), article number 5700. doi: 10.3390/app13095700.

[3] Argyridou, E., Nifakos, S., Laoudias, C., Panda, S., Panaousis, E., Chandramouli, K., Navarro-Llobet, D., Mora Zamorano, J., Papachristou, C., & 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, article number e41294. doi: 10.2196/41294.

[4] Bender, S., Horn, S., Loewenstein, G., & Roberts, O. (2024). Phishing feedback: Just-in-time intervention improves online security. *Behavioural Public Policy*, 10(3), 527-539. doi: 10.1017/bpp.2024.19.

[5] Bognár, L. (2025). Predicting cybersecurity incidents via self-reported behavioral and psychological indicators: A stratified logistic regression approach. *Journal of Cybersecurity and Privacy*, 5(3), article number 67. doi: 10.3390/jcp5030067.

[6] 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 number 588. doi: 10.3390/educsci14060588.

[7] Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring age and gender differences in ICT cybersecurity behaviour. *Human Behavior and Emerging Technologies*, 2022(1), article number 2693080. doi: 10.1155/2022/2693080.

[8] Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small- and medium-sized enterprises. *Computer Science Review*, 50, article number 100592. doi: 10.1016/j.cosrev.2023.100592.

[9] Desolda, G., Ferro, L.S., Marrella, A., Catarci, T., & Costabile, M.F. (2021). Human factors in phishing attacks: A systematic literature review. *ACM Computing Surveys*, 54(8), article number 173. doi: 10.1145/3469886.

[10] European Commission. (2021). *Ethics and Data Protection*. Retrieved from https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf.

[11] Hanus, B., Windsor, J.C., & Wu, Y. (2018). Definition and multidimensionality of security awareness: Close encounters of the second order. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, 49(1), 103-133. doi: 10.1145/3210530.3210538.

[12] Hasegawa, K., O'Brien, N., Prendergast, M., Bompani, N., Peiris, D., & Darzi, A. (2024). Cybersecurity interventions in health care organizations in low- and middle-income countries: Scoping review. *Journal of Medical Internet Research*, 26, article number e47311. doi: 10.2196/47311.

[13] Hong, Y., & Furnell, S. (2021). Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications*, 57, article number 102710. doi: 10.1016/j.jisa.2020.102710.

[14] Karayel, T., Aktaş, B., & Akbıyık, A. (2025). Human factors in remote work: Examining cyber hygiene practices. *Information & Computer Security*, 33(1), 96-116. doi: 10.1108/ICS-11-2023-0215.

[15] Kennison, S.M., & Chan-Tin, E. (2020). Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. *Frontiers in Psychology*, 11, article number 546546. doi: 10.3389/fpsyg.2020.546546.

[16] Khadka, K., & Ullah, A.B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security*, 24, article number 119. doi: 10.1007/s10207-025-01032-0.

[17] Khan, N.F., Ikram, N., & Saeed, S. (2022). The cybersecurity behavioral research: A tertiary study. *Computers & Security*, 120, article number 102826. doi: 10.1016/j.cose.2022.102826.

[18] Kovalchuk, D. (2025). Utilising large language models for automated real-time cyber threat analysis. *Bulletin of Cherkasy State Technological University*, 30(1), 48-58. doi: 10.62660/bcstu/1.2025.48.

[19] Lee, C.S., & Kim, D. (2023). Pathways to cybersecurity awareness and protection behaviors in South Korea. *Journal of Computer Information Systems*, 63(1), 94-106. doi: 10.1080/08874417.2022.2031347.

[20] Mayer, P., Zou, Y., Lowens, B.M., Dyer, H.A., Le, K., Schaub, F., & Aviv, A.J. (2023). Awareness, intention, (in)action: Individuals' reactions to data breaches. *ACM Transactions on Computer-Human Interaction*, 30(5), article number 77. doi: 10.1145/3589958.

[21] Morrison, B., Coventry, L., & Briggs, P. (2021). How do older adults feel about engaging with cyber-security? *Human Behavior and Emerging Technologies*, 3(5), 1033-1049. doi: 10.1002/hbe2.291.

[22] Morrow, E. (2024). Scamming higher ed: An analysis of phishing content and trends. *Computers in Human Behavior*, 158, article number 108274. doi: 10.1016/j.chb.2024.108274.

[23] Nguyen, B.H., & Le, H.N.Q. (2024). Investigation on information security awareness based on KAB model: The moderating role of age and education level. *Information & Computer Security*, 32(5), 598-612. doi: 10.1108/ICS-09-2023-0152.

[24] Polishchuk, V., & Sehlianyk, V. (2026). Dataset of 315 respondents on digital security behavior across socio-demographic groups. *Zenodo*. doi: 10.5281/zenodo.18953401.
[25] Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, 136, article number 103585. doi: 10.1016/j.cose.2023.103585.
[26] 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 number e14234. doi: 10.1016/j.heliyon.2023.e14234.
[27] Skare, M., Gavurova, B., & Polishchuk, V. (2026). Information-analytical system for evaluating artificial intelligence readiness and adoption in enterprises: A policy framework. *International Entrepreneurship and Management Journal*, 22, article number 52. doi: 10.1007/s11365-026-01187-9.
[28] Šolić, K., Velki, T., Fosić, I., & Vuković, M. (2024). Study on information security awareness using the behavioral-cognitive internet security questionnaire. *Acta Polytechnica Hungarica*, 21(4), 49-68. doi: 10.12700/APH.21.4.2024.4.3.
[29] van Steen, T., & Deeleman, J.R.A. (2021). Successful gamification of cybersecurity training. *Cyberpsychology, Behavior, and Social Networking*, 24(9), 593-598. doi: 10.1089/cyber.2020.0526.
[30] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H.N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1), 82-97. doi: 10.1080/08874417.2020.1712269.

Нечітка модель оцінювання поведінкового компоненту цифрової безпеки населення різних соціально-демографічних груп

Володимир Поліщук

Доктор технічних наук, професор
Технічний університет у Кошицях
04121, вул. Рампова, 7, м. Кошице, Словаччина
Ужгородський національний університет
88000, пл. Народна, 3, м. Ужгород, Україна
https://orcid.org/0000-0003-4586-1333

Василь Сегляник

Аспірант
Ужгородський національний університет
88000, пл. Народна, 3, м. Ужгород, Україна
https://orcid.org/0009-0005-9958-3713

Анотація. Актуальність дослідження зумовлена зростанням кіберзагроз у цифровому середовищі та необхідністю розроблення методів оцінювання поведінкового компоненту цифрової безпеки з урахуванням відмінностей у цифровій грамотності й досвіді використання технологій різними соціально-демографічними групами. Метою дослідження було обґрунтування підходу до оцінювання рівня безпечної поведінки користувачів у цифровому середовищі з урахуванням соціально-демографічних відмінностей населення. Для досягнення поставленої мети використано методи інтелектуального аналізу знань, теорію нечітких множин, багатовимірні функції належності та методи соціологічного аналізу даних. Було розроблено інформаційну модель оцінювання поведінкового компоненту цифрової безпеки населення, яка ґрунтується на системі критеріїв безпечної взаємодії користувачів із цифровим середовищем. Сформовано групи показників, що відображають рівень обізнаності громадян щодо кіберзагроз, практики використання засобів захисту персональних даних та поведінкові особливості під час взаємодії з цифровими ресурсами. Запропоновано нечіткий підхід визначення інтегрального рівня цифрової безпеки на основі багатовимірних функцій належності, який дозволяє інтегрувати кількісні та якісні показники оцінювання та отримувати числові й лінгвістичні оцінки рівня безпечної поведінки користувачів. Проведено верифікацію моделі на основі даних анкетного опитування 315 респондентів різних соціально-демографічних груп населення. Практична цінність одержаних результатів полягає у можливості інтеграції розробленої моделі в системи підтримки прийняття рішень, призначені для моніторингу рівня цифрової безпеки населення, сегментації соціально-демографічних груп за рівнем кіберризику та обґрунтування адресних управлінських, освітніх і профілактичних заходів щодо підвищення цифрової грамотності та безпечної поведінки користувачів

Ключові слова: кіберзагрози; безпечна цифрова поведінка; нечітка логіка; цифрова грамотність; багатокритеріальне оцінювання; функції належності; підтримка прийняття рішень