Scientific Journal of the Ternopil National Technical University
2026, vol. 121, no. 1, pp. 107–118,
ISSN: 2522-4433 Print, ISSN: 2522-4441 Online
https://doi.org/10.33108/visnyk_tntu2026.01.107

Submitted: 2025-11-08 | Revised: 2026-02-01 | Accepted: 2026-03-24

A fuzzy framework for assessing the level of cognitive and operational readiness of regional citizens to ensure their own digital security

Volodymyr Polishchuk [1,2*], Vasyl Sehlianyk [3]

[1] Technical University of Kosice, Slovakia, volodymyr.polishchuk@uzhnu.edu.ua

[2] Uzhhorod National University, Ukraine, volodymyr.polishchuk@uzhnu.edu.ua

[3] Uzhhorod National University, Ukraine, vasyl.sehlianyk@uzhnu.edu.ua

***** Corresponding author volodymyr.polishchuk@uzhnu.edu.ua

Abstract: *Citizens' growing involvement in the digital environment increases exposure to cyber risks caused by the human factor. However, existing assessment approaches mainly focus on technical cybersecurity capacity or general digital literacy and do not comprehensively capture both cognitive awareness and the ability to make correct decisions in typical cyber situations. The purpose of the study is to develop and verify a fuzzy framework for assessing the level of cognitive and operational readiness of citizens of a region to ensure their own digital security. The information base was formed using a questionnaire survey of citizens and two information methods: self-assessment of cognitive cybersecurity awareness on a ten-point scale and assessment of applied cyberliteracy through single-answer test questions. An integral assessment was obtained using a fuzzy model with multidimensional membership functions and a fuzzy rule base. The proposed framework was tested on real data from 315 respondents in the Transcarpathian region collected during March–June 2025. The resulting integral indicator of cognitive and operational readiness was 0.67, which corresponds to a stable average level of population readiness to ensure personal digital security. The proposed framework provides a comprehensive, reproducible, and scalable assessment of citizens' readiness for digital security and can be used to identify high-risk groups and support educational, preventive, and managerial decision-making at regional and national levels.*

Keywords: *information security of citizens; cognitive awareness; applied cyberliteracy; cybersecurity; fuzzy modeling; decision support; fuzzy sets*

1. INTRODUCTION

In today's conditions of intensive digital transformation of society, information and communication technologies penetrate almost all spheres of human life, creating new opportunities for socio-economic development, while at the same time generating growing risks associated with the security of personal data, digital services, and information resources. The increase in the number of cyber incidents, the spread of social engineering, and the increasing complexity of digital threats actualize the need for a systematic approach to assessing the readiness of the population to safely interact with the digital environment.

The relevance of developing a methodological framework for assessing the cognitive and operational readiness of citizens to ensure digital security is determined by the rapid digitalization of society and the growing role of the human factor in cyber incidents. Despite the existence of international indices and national statistical indicators, most of them are focused mainly on the technical state of cyber defense, the level of digital infrastructure, or the general digital literacy of

the population, without considering the comprehensive combination of cognitive awareness and the ability of citizens to make correct decisions in typical cyber situations.

To analyze the scientific background of this study, the literature can be grouped into several substantive strands related to cognitive cybersecurity awareness, applied cyberliteracy, and regional digital resilience. These include cognitive awareness and behavioral models [1–2], applied cyberliteracy and operational readiness [3–4], fuzzy modeling and decision support systems for assessment under uncertainty [5–6], and cyber maturity with regional cyber resilience, where citizen readiness is viewed as a component of overall regional security [7–8].

Cognitive awareness, behavioral models, and the human factor in cybersecurity. In modern cybersecurity research, increasing attention is paid to cognitive and behavioral factors that determine the ability of users to perceive digital threats and make informed protective decisions. Such approaches allow us to move from a purely technical understanding of cybersecurity to a human-centered paradigm. At the same time, it has been proven that subjective factors, in particular life satisfaction and emotional resilience, indirectly affect the level of cyberawareness and adherence to safe behavior [9]. A separate direction is formed by empirical studies of cyber awareness in various socio-professional groups, among remote workers, employees of public organizations, and educational institutions. These works prove that the level of cognitive awareness significantly affects the readiness of users to comply with security policies and respond to incidents [10–12]. The results obtained create a theoretical basis for the formation of indicators of the cognitive component of the population's readiness to ensure their own digital security. In addition, the impact of digital communications and mobile technologies on the formation of the population's cyber resilience has been confirmed based on adaptive regression models [13].

Applied Cyber Literacy and User Operational Readiness. Applied cyber literacy is considered the ability of users not only to be aware of threats but also to effectively apply knowledge in practice when interacting with the digital environment. A few studies have focused on assessing real-world skills of secure behavior, such as password management, recognizing phishing attacks, responding to incidents, and adhering to organizational policies [3–4]. The use of multi-level analytical approaches allows for quantitative measurement of the level of applied cyber literacy. Systematic reviews show that the effectiveness of cybersecurity training significantly depends on the form of presentation of the material and the mechanisms of behavioral change [14]. Applied cyber literacy is a dynamic construct shaped by training, experience, and social context, with operational readiness strongly linked to users' participation in digital ecosystems and collective security practices [15]. In smart cities, where citizens function as active elements of cyber-physical systems, this underscores the need to integrate applied indicators into comprehensive readiness assessment models [16].

Fuzzy modeling in this study is considered not as a separate substantive area of cybersecurity research, but as a methodological tool for processing and integrating heterogeneous assessment data. Recent studies show that fuzzy logic, multi-criteria methods, and related intelligent techniques are effective for analyzing cybersecurity phenomena under uncertainty and incomplete information [5–6, 17]. Such approaches enable the integration of quantitative and qualitative indicators, improve interpretability, and support the construction of integral assessment indices [18–24]. Therefore, in the present paper fuzzy modeling serves as the methodological basis for combining the results of two information methods – cognitive cybersecurity awareness assessment and applied cyberliteracy assessment – into a single integral indicator of citizens' cognitive and operational readiness.

Cyber Maturity, Regional Security and Strategic Governance. Within the fourth area, cybersecurity is considered a component of regional and urban development, which requires a systematic assessment of the level of maturity and readiness of social and infrastructure systems. Cyber maturity research offers various indicator models that consider organizational, technological, and human aspects of security [8, 25]. It is emphasized that excessive digital

control and privacy violations can reduce trust and negatively affect the long-term cyber resilience of society [26]. Such approaches are relevant for analyzing the state of digital security at the regional level. At the same time, works dedicated to smart regions and national infrastructure use fuzzy models of strategic planning and risk assessment, which allow for the formation of recommendations for public policy and governance [7, 27 28]. In this context, assessing the cognitive and operational readiness of citizens is an important element of ensuring sustainable regional digital security. Additionally, situational awareness and big data analysis approaches are used to monitor the security status of network environments [29 30].

The literature review indicates that citizens' readiness for digital security has been studied through several related but largely separate perspectives, including cybersecurity awareness, practical cyber skills, and regional cyber resilience. However, the existing studies do not provide a formalized and reproducible framework that integrates cognitive cybersecurity awareness and applied cyberliteracy into a single assessment of citizens' cognitive and operational readiness at the regional level. This gap determines the novelty of the present paper, which proposes an integrated fuzzy framework for obtaining both quantitative and linguistic assessment results that can support educational, preventive, and managerial decision-making.

The purpose of the study is to develop and verify a fuzzy framework for assessing the level of cognitive and operational readiness of citizens of a region to ensure their own digital security and to provide a basis for substantiated managerial, educational, and preventive recommendations in the field of digital security.

2. MATERIALS AND METHODS

The object of the study is considered within the territory R, which can cover the city, regional, or national level. The population (respondents) living in this territory is formalized as a set $C = \{c_1; c_2; \dots; c_n\}$. The goal is to assess the level of cognitive and operational readiness of citizens to ensure their own digital security. To form the information base of the study, it is planned to conduct a survey of respondents. Input data is collected using a text questionnaire developed in accordance with the K criteria system. Based on the questionnaire, according to the evaluation criteria, two information methods for processing input data are proposed, namely: K_{CAC} – an information method for assessing cognitive awareness of cybersecurity; K_{ACL} – an information method for assessing applied cyber literacy of citizens. The processed input data using information methods is used for calculations by a fuzzy model for assessing the level of cognitive and operational readiness of citizens to ensure digital security – M_{COR}. The formal formulation of the framework for assessing the level of cognitive and operational readiness of citizens of the region to ensure their own digital security is proposed to be presented in the form of the following operator:

$$\theta: (R, C, K_{CAC}, K_{ACL}, M_{COR}) \to Y(f). \quad (1)$$

Here, θ denotes the integrated assessment operator that transforms the input data, criteria system, and processing models into the final output vector containing quantitative and linguistic characteristics of citizens' cognitive and operational readiness for digital security.

Based on the input data R, C and their processing models $K_{CAC}, K_{ACL}, M_{COR}$ the operator θ outputs the output value $Y(f) = (I_{CAC}, I_{ACL}, R_{COR}, L_{COR})$. The obtained output values contain the following content: I_{CAC} – index of cognitive awareness of cybersecurity; I_{ACL} – index of applied cyber literacy of citizens; R_{COR} – integral assessment of the level of cognitive and operational readiness of citizens of the region to ensure their own digital security; L_{COR} – linguistic knowledge of cognitive and operational readiness of citizens of the region to ensure their own digital security.

For a visual presentation of the study, a structural diagram of the fuzzy model is given (Fig. 1).

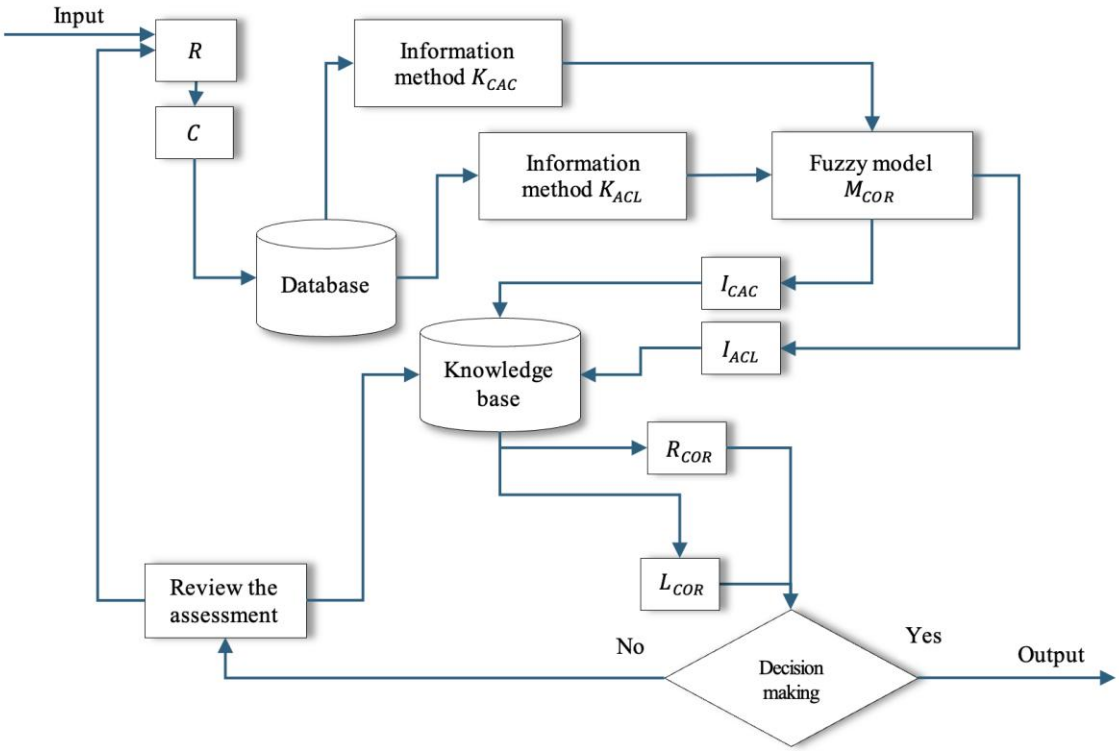

Figure 1. Flowchart of assessment framework.

At the input of the system, input data about the territory R and the set of respondents C, are formed, which fill the database based on the results of a questionnaire survey developed in accordance with the system of criteria K. Further data processing is carried out by two information methods: K_{CAC}, which provides an assessment of the level of cognitive awareness of citizens in the field of cybersecurity, and K_{ACL}, aimed at determining the level of their applied cyber literacy.

The results of the information methods are fed into the fuzzy model M_{COR}, which performs integral aggregation of indicators and forms an assessment of cognitive and operational readiness. The obtained output parameters provide both quantitative and linguistic interpretations of the level of preparedness, which form the basis for decision-making, review of the assessment, and determination of the result. The decision-making block shown in Figure 1 is not an independent computational stage of the model, but a stage of practical interpretation and use of the obtained results. Based on the integral indicator $R_{COR}$and its linguistic interpretation L_{COR}, this block supports the formulation of managerial, educational, and preventive recommendations aimed at improving citizens' digital security readiness at the regional level. Thus, the final outputs of the proposed framework are not limited to numerical assessment but also serve as a basis for substantiated decision support. In general, the scheme formalizes the assessment operator θ, which provides a systematic and reproducible evaluation of citizens' cognitive and operational readiness to ensure digital security.

K_{CAC} – information method for assessing cognitive awareness of cybersecurity

At the initial stage of the study, an array of input data is formed using an information assessment method. For this, an open system of criteria is used, which allows examining the level of cognitive awareness of citizens in the field of cybersecurity. Respondents self-assess their knowledge on a ten-point scale, where the value 1 corresponds to an insignificant level of expertise, and the value 10 corresponds to a significant one. Intermediate values of the scale are interpreted as average levels of knowledge.

K_{C1} – How aware are you of what to do if you discover a suspicious app or program on your device?

K_{C2} – How familiar are you with the term «cybercrime»?

K_{C3} – How do you rate your knowledge of the methods by which cybercriminals can steal personal data?

K_{C4} – How knowledgeable are you about cyberbullying and methods for protecting against it?

K_{C5} – How do you rate your knowledge regarding your experience or likelihood of becoming a victim of cybercrime (data theft, fraud)?

K_{C6} – How well do you understand who is responsible for protecting personal data: the citizen, the company, or the government?

K_{C7} – How do you rate your knowledge of cybercrime prevention at the individual level?

Based on the survey results, a range of input data is compiled, presented as point estimates according to the K_{Cp}criteria. The corresponding values are denoted by e_{Cp}, where p – is the criterion number $\left(p = \overline{1,l.} \right)$. To ensure the comparability of the obtained data, a transition is made from quantitative point estimates to normalized indicators, which requires the preliminary formation of a generalized integral estimate:

$$\alpha(c_i) = \sum_{p=1}^{l} e_{Cp}(c_i),\ i = \overline{1,n.} \qquad (2)$$

where i – number of the respondent, $i = \overline{1,n.}$

The proposed information method provides a formalized assessment of citizens' cognitive awareness in the field of cybersecurity, based on an open system of criteria. Self-assessment on a ten-point scale enables the quantification of individual perceptions, forming a reliable information base for further fuzzy modeling and integral assessment of cognitive and operational readiness for digital security.

K_{ACL} – information method for assessing applied cyberliteracy of citizens

To assess the level of cyber literacy among citizens, a set of questions with fixed answer options is proposed, each with only one correct answer. If the correct choice is made, the respondent is awarded 1 point. A set of open-ended questions is provided that can be used to implement the assessment.

K_{A1} – Which of the following passwords do you think is the most secure?

K_{A2} – A technician from the bank you use calls you and asks for your card password due to technical work. What will be your reaction?

K_{A3} – A close relative calls you from a different number and asks you to urgently transfer money due to a car accident or sudden deterioration in your health. What will be your reaction?

K_{A4} – What do you think is the best way to prevent illegal use of Bluetooth?

K_{A5} – What password storage practice is the most secure and convenient?

K_{A6} – What do you understand by two-factor authentication?

K_{A7} – On Facebook, you receive a friend request from an unknown person with a blank and newly created profile. Will you accept this request?

K_{A8} – Do you check the accuracy of facts or news through several independent sources?

K_{A9} – Do you explain to your children the dangers of sharing private information online?

K_{A10} – Do you find accessing your bank account using a password and an additional verification factor (SMS, call, fingerprint) too complicated?

K_{A11} – Is it safe to make bank transfers over an open Wi-Fi network (e.g. in a coffee shop)?

K_{A12} – How often do you change your bank account password?

K_{A13} – Do you use the same passwords for different applications or services?

K_{A14} – What should you do if you receive an email saying you won a lottery you didn't enter?

K_{A15} – How can you tell if a website is safe for entering personal information?

K_{A16} – What do you do if you suspect your account has been hacked?

K_{A17} – What, in your opinion, is the main function of antivirus software?

Similarly, based on the results of the survey of respondents, an array of input data is formed, denoted by e_{Ak}, where k – is the question number $\left(k = \overline{1,h.}\right)$. Next, a generalized integral estimate is formed:

$$\beta(c_i) = \sum_{k=1}^{h} e_{Ak}(c_i),\ i = \overline{1,n.} \quad (3)$$

where i – number of the respondent, $i = \overline{1,n.}$

The K_{ACL} information method provides a formalized assessment of the level of applied cyber literacy of citizens based on test questions with a single correct answer. The scoring scheme enables the objective recording of practical skills related to safe behavior in the digital environment, and the aggregation of results into an integral indicator ensures the comparability of cyber literacy levels between respondents. The obtained data create a reliable basis for integration with cognitive indicators within the framework of a comprehensive assessment of citizens' readiness for digital security.

M_{COR} – a fuzzy model for assessing the level of cognitive and operational readiness of citizens to ensure digital security

Firstly, the input data is fuzzified using S-shaped membership functions, as the increase in the score corresponds to a rise in the level of cognitive awareness and applied cyberliteracy. Membership functions are formed separately for cognitive awareness and applied cyberliteracy using a quadratic S-spline, the parameters of which are determined by the minimum and maximum values of the scores. The choice of S-shaped membership functions is обусловлена monotonic nature of both assessment dimensions: higher questionnaire scores correspond to higher levels of cognitive awareness and applied cyberliteracy. In this context, the S-shape provides a smooth transition from low to high membership values and is appropriate for modeling gradual accumulation of readiness rather than abrupt threshold changes. The parameters of the functions were specified based on the admissible score ranges defined by the questionnaire structure, namely the minimum and maximum attainable values for each assessment component. Thus, the parameterization was primarily determined by the formal scoring scheme of the instrument and by the methodological need to normalize heterogeneous indicators to the interval $[0;\ 1]$. At the present stage, expert knowledge was used at the stage of constructing the criteria system and interpreting the resulting linguistic levels, whereas the parameters of the membership functions themselves were not obtained through a separate expert elicitation procedure or statistical fitting, but were set analytically from the observed score domains.

$$\mu_{CAC}(c_i) = \begin{cases} 0, & \alpha(c_i) \le 7; \\ \dfrac{(\alpha(c_i) - 7)^2}{1922}, & 7 < \alpha(c_i) \le 38; \\ 1 - \dfrac{\left(69 - \alpha(c_i)\right)^2}{1922}, & 38 < \alpha(c_i) < 69; \\ 1, & \alpha(c_i) = 69. \end{cases} \quad (4)$$

$$\mu_{ACL}(c_i) = \begin{cases} 0, & \beta(c_i) \le 1; \\ \dfrac{(\beta(c_i) - 1)^2}{128}, & 1 < \beta(c_i) \le 8; \\ 1 - \dfrac{\left(17 - \beta(c_i)\right)^2}{128}, & 8 < \beta(c_i) < 17; \\ 1, & \beta(c_i) = 17. \end{cases} \quad (5)$$

The obtained estimates $\{\mu_{CAC}(c_i),\ \mu_{ACL}(c_i)\} \in [0;1]$ are normalized and characterize the corresponding levels of cognitive awareness and applied cyberliteracy among citizens. The

notation is intentionally kept in generalized form to preserve the adaptability of the framework to other numbers of criteria and test items, while the terminal intervals in the membership functions are included for mathematical completeness of the model.

Next, the cognitive cybersecurity awareness index is determined at the level of the studied region:

$$I_{CAC}(R) = \frac{1}{n}\sum_{i=1}^{n} \mu_{CAC}(c_i). \quad (6)$$

The resulting $I_{CAC} \in [0; 1]$ – is the index of cognitive awareness of cybersecurity, which characterizes the level of knowledge and understanding among citizens of the main threats in the digital environment, methods for recognizing them, and basic principles of personal information protection. This index is normalized and can be interpreted as follows:

$I_{CAC} \in [0; 0{,}3)$ – low level characterizes fragmentary, superficial representations.

$I_{CAC} \in [0{,}3;\ 0{,}7)$ – medium level reflects understanding of the main threats and responsibilities.

$I_{CAC} \in [0{,}7; 1]$ – a high level characterizes systemic awareness of risks, roles and prevention.

Similarly, the index of applied cyberliteracy is derived at the level of the studied region:

$$I_{ACL}(R) = \frac{1}{n}\sum_{i=1}^{n} \mu_{ACL}(c_i). \quad (7)$$

As a result, $I_{ACL} \in [0; 1]$ – is obtained - the index of applied cyber literacy of citizens, which characterizes the level of practical skills of safe behavior in the digital environment, in particular, the ability to recognize cyber threats, correctly respond to fraudulent actions, and apply effective means of protecting personal data. The index of applied cyber literacy of citizens reflects the following:

- $I_{ACL} \in [0; 0{,}3)$ – low level, characterized by the inability to recognize cyber threats and a tendency to choose dangerous actions.
- $I_{ACL} \in [0{,}3; 0{,}7)$ – average level, which reflects the presence of basic knowledge of cybersecurity rules, but their inconsistent or incorrect application in practice.
- $I_{ACL} \in [0{,}7;\ 1]$ – high level, characterized by a systemic understanding of cyber threats and the ability to choose correct and safe actions in typical digital situations.

The justification of the ranges for I_{CAC} and I_{ACL} is based on their normalization to the interval $[0; 1]$ and on the use of a three-level linguistic interpretation scale. In this study, the cut-off points 0.3 and 0.7 were adopted as analytical boundaries separating insufficient, moderate, and sufficiently expressed levels of the corresponding component. This partition does not rely on external regulatory thresholds, but on the need to provide a clear and reproducible interpretation of the obtained integral indices within the proposed assessment framework.

The next stage is the development of an integrated assessment of the level of cognitive and operational readiness of citizens to ensure digital security.

As a result, two normalized indices of cognitive awareness and applied cyberliteracy I_{CAC} та I_{ACL} are obtained. To form an integral assessment of the level of cognitive and operational readiness of citizens in the studied region to ensure digital security, it is proposed to use multidimensional membership functions within the framework of intellectual analysis of knowledge. Given the need to model uncertainties of the «mean value» type in the two-dimensional space of estimates $[0; 1]$, it is advisable to use a conical or pyramidal membership function. These functions are characterized by the fact that with the increase in the values of the input variables to the maximum level, the integral estimate asymptotically approaches 1. In particular, the pyramidal membership function in a two-dimensional space can be presented in the following form:

$$R_{COR}(R) = \max\left\{\left(1 - \frac{1}{2}(|I_{CAC} - 1| + |I_{ACL} - 1|)\right); 0\right\}. \quad (8)$$

where is the scaling by coordinates – $(2; 2)$, the center of the base – $(1; 1)$.

Thus, an integrated assessment of the level of cognitive and operational readiness of citizens to ensure their own digital security [0; 1] within the studied region is obtained, which makes it possible to conduct a comprehensive comparative analysis between individual population groups, identify high-risk areas, and justify priority areas of educational and preventive measures in the field of cybersecurity.

The approach of the integral index to a value of 1 indicates a high average level of cognitive and operational readiness among the population to ensure digital security in the studied region, which is reflected in the dominance of citizen profiles characterized as «digitally mature» and «practically competent». Additionally, it reduces the region's vulnerability to mass cyber incidents associated with the influence of the human factor.

At the final stage, the L_{COR}, indicator is formed, reflecting linguistic knowledge regarding the level of cognitive and operational readiness of the region's citizens to ensure their own digital security. For this purpose, it is proposed to utilize linguistic levels of cognitive awareness of cybersecurity and applied cyber literacy among citizens, based on which a fuzzy knowledge base is formed to support management decisions at the state level. It is proposed to build a fuzzy knowledge base consisting of systems of logical statements – «If-Then, Otherwise», which connect the values of the input linguistic levels (I_{CAC}, I_{ACL}) with one of the possible linguistic interpretations of L_{COR}:

IF I_{CAC} = High and I_{ACL} = Low THEN L_{COR} ={ Citizens of the region are well aware of the types and nature of cyber threats, but demonstrate limited ability to make the right choice of actions in practical situations} ELSE

IF I_{CAC} = High and I_{ACL} = Average THEN L_{COR} ={ Characterized by awareness of basic cyber risks and partial application of knowledge in everyday digital activities} ELSE

IF I_{CAC} = High and I_{ACL} = High THEN L_{COR} ={ Citizens possess systemic knowledge and consistently make correct decisions that ensure a high level of digital security} OTHERWISE

IF I_{CAC} = Medium and I_{ACL} = Low THEN L_{COR} ={ Knowledge about cybersecurity is incomplete and unsystematic, which leads to frequent errors in choosing actions in the digital environment} OTHERWISE

IF I_{CAC} = Medium and I_{ACL} = Middle THEN L_{COR} ={ Stable average level of knowledge and decisions sufficient for basic personal digital security} OTHERWISE

IF I_{CAC} = Medium and I_{ACL} = High THEN L_{COR} ={ Citizens demonstrate the ability to act safely in typical situations even with incomplete understanding of threat mechanisms} OTHERWISE

IF I_{CAC} = Low and I_{ACL} = Low THEN L_{COR} ={ Citizens are characterized by a lack of basic knowledge and an inability to make safe decisions, which forms a critical risk zone in the region} OTHERWISE

IF I_{CAC} = Low and I_{ACL} = Middle THEN L_{COR} ={ Citizens apply cautious behavior without a clear understanding of causes and consequences, relying mainly on intuition} OTHERWISE

IF I_{CAC} = Low and I_{ACL} = High THEN L_{COR} ={ Citizens implement mostly safe actions, but do not have a systematic understanding of digital security principles}.

Thus, all possible cases of formulated knowledge base rules have been exhausted.

3. RESULTS AND THEIR DISCUSSION

The proposed framework for assessing the level of cognitive and operational readiness of citizens in the region to ensure their own digital security was verified and tested using real data from the population of the Transcarpathian region [31]. From March to June 2025, a large-scale questionnaire survey was conducted, within which data were collected from 315 respondents using a broader questionnaire consisting of 49 questions. At the same time, for

the purposes of the present study and the construction of the proposed assessment model, only 24 questions were selected from the full survey instrument, including 7 questions for assessing cognitive cybersecurity awareness and 17 questions for assessing applied cyberliteracy. The collection of empirical data aimed to study the population's attitude towards information security issues and the characteristics of their interaction with the digital environment. The obtained statistical data meet the requirements for forming a representative sample, which is confirmed by the respondents' membership in the target population and their diverse socio-demographic characteristics. Among the respondents, 60% are men and 40% are women, while 98.5% of respondents are of working age and actively use computer information technologies.

The developed framework was verified on the full dataset. To enable replication of the experiments by other researchers, an example of the evaluation is provided. Individual fragments of the input data are presented in Table 1, while the whole dataset is publicly available [31].

After collecting input data from respondents, a generalized integral estimate is formed according to formulas (2) and (3). Next, the input data is fuzzified using S-shaped membership functions, according to formulas (4) and (5):

c_1: $\alpha(c_1)$ =51; $\mu_{CAC}(c_1)$ =0.831; $\beta(c_1)$ =5; $\mu_{ACL}(c_1)$ =0.125.
c_2: $\alpha(c_2)$ =59; $\mu_{CAC}(c_2)$ =0.948; $\beta(c_2)$ =8; $\mu_{ACL}(c_2)$ =0.383.
c_3: $\alpha(c_3)$ =39; $\mu_{CAC}(c_3)$ =0.532; $\beta(c_3)$ =14; $\mu_{ACL}(c_3)$ =0.93.
……
c_{315}: $\alpha(c_{315})$ =41; $\mu_{CAC}(c_{315})$ =0.592; $\beta(c_{315})$ =12; $\mu_{ACL}(c_{315})$ =0.805.

Table 1. Input data fragments.

Information method	Criteria	c_1	c_2	c_3	…	c_{315}
G_1	K_{C1}	8	9	4	…	6
	K_{C2}	8	8	3	…	5
	…	…	…	…	…	…
	K_{C7}	7	9	7	…	5
G_2	K_{A1}	0	1	1	…	1
	K_{A2}	1	0	1	…	0
	…	…	…	…	…	…
	K_{A17}	0	1	1	…	0

Next, using formula (6), the index of cognitive awareness of cybersecurity at the level of the Transcarpathian region is determined: $I_{CAC}(R)$ =0.676. The resulting index $I_{CAC} \in$ [0,3; 0,7) is interpreted as the average level.

Similarly, the index of applied cyberliteracy is derived using the formula (7): $I_{ACL}(R)$ =0.664. The index of applied cyberliteracy $I_{ACL} \in$ [0,3; 0,7) of citizens also reflects the average level.

Next, an integral assessment of the level of cognitive and operational readiness of citizens to ensure their own digital security within the studied region is obtained using the formula (8): $R_{COR}(R) = 0.67$.

At the final stage, linguistic knowledge L_{COR}, is formed, which reflects linguistic knowledge regarding the level of cognitive and operational readiness of citizens of the region to ensure their own digital security: L_{COR} = { Stable average level of knowledge and decisions sufficient for basic provision of personal digital security}.

The research is based on the apparatus of fuzzy set theory, fuzzy logic, methods of intellectual analysis of knowledge, and expert assessment. The use of such mathematical apparatus enables us to adequately account for the uncertainty and subjectivity of input data, a

characteristic of socially oriented research. Also, it facilitates the formalization of heterogeneous indicators into a single, integral assessment of the level of cognitive and operational readiness of citizens to ensure digital security.

The developed framework has high practical value, as it enables the systematic and reproducible assessment of the population's cognitive and operational readiness to ensure digital security at various territorial levels. This allows for the identification of high-risk groups and the formulation of substantiated management, educational, and preventive solutions, considering regional characteristics.

The limitations of the study are related to the use of fuzzy modeling, in particular, the choice of types and parameters of membership functions, which may lead to some ambiguity in the evaluation results. In addition, the evaluation results depend on the representativeness of the sample and the selected system of criteria, which limits the possibility of directly generalizing the results to all regions without additional calibration of the model.

4. CONCLUSIONS

For the first time, a framework has been developed that creates a formalized approach to assessing the cognitive and operational readiness of citizens to ensure digital security, based on the integration of cognitive awareness indices and applied cyberliteracy using fuzzy multidimensional membership functions. Unlike existing approaches, the proposed framework enables the simultaneous acquisition of quantitative and linguistic results, allows for consideration of the uncertainty in social data, and forms a new methodological basis for systematic and reproducible analysis of the population's readiness for safe interaction with the digital environment at both regional and national levels.

Practical results enable a comprehensive assessment of the cognitive and operational readiness of citizens to ensure digital security, identify high-risk groups, and inform management, educational, and preventive measures, considering regional characteristics.

Further research by the authors involves expanding the collection of empirical data to other regions of Ukraine to test the framework in additional areas. The mechanisms for tuning the model will also be improved, as well as the development of software based on the proposed framework to automate the assessment process and support management decisions in the field of digital security.

Author Contributions: Conceptualization: V.P. (Volodymyr Polishchuk); Methodology: V.P.; Software: V.S. (Vasyl Sehlianyk); Validation: V.P., V.S.; Formal analysis: V.P., V.S.; Writing – original draft preparation: V.P., V.S.; Writing – review and editing: V.P., V.S.; Supervision: V.P.

Conflicts of Interest: All authors declare that there are no competing interests.

Data Availability Statement. The data that support the findings of this study are openly available in Zenodo: Polishchuk V., Sehlianyk V. *Data from 315 respondents to assess the level of cognitive and operational readiness of citizens of the region to ensure their own digital security (Ukraine)* [Data set], 2026, at https://doi.org/10.5281/zenodo.19692560.

Declaration of Generative AI and AI-assisted technologies in the writing process: The authors declare that no generative AI or AI-assisted technologies were used in the writing of this manuscript.

REFERENCES

[1] U. Kiran, N.F. Khan, H. Murtaza, A. Farooq, H. Pirkkalainen, Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory, Computers & Security. 149 (2025) 104204. https://doi.org/10.1016/j.cose.2024.104204.

[2] D. Baltuttis, T. Teubner, M.T.P. Adam, A typology of cybersecurity behavior among knowledge workers, Computers & Security. 140 (2024) 103741. https://doi.org/10.1016/j.cose.2024.103741.

[3] R.C. Chanda, A. Vafaei-Zadeh, H. Hanifah, D. Nikbin, Assessing cybersecurity awareness among bank employees: A multi-stage analytical approach using PLS-SEM, ANN, and fsQCA in a developing country context, Computers & Security. 125 (2025) 104208. https://doi.org/10.1016/j.cose.2024.104208.

[4] H. Taherdoost, A critical review on cybersecurity awareness frameworks and training models, Procedia Computer Science. 235 (2024) 1649–1663. https://doi.org/10.1016/j.procs.2024.04.156.

[5] M. Güler, G. Büyüközkan, Cybersecurity maturity assessment using an incomplete hesitant fuzzy AHP method and Bonferroni means operator, Expert Systems with Applications. 282 (2025) 127268. https://doi.org/10.1016/j.eswa.2025.127268.

[6] O. Soner, Modeling and analyzing cybersecurity risk propagation in ports using fuzzy cognitive maps: System sensitivity to key threat factors, Ocean & Coastal Management. 270 (2025) 107857. https://doi.org/10.1016/j.ocecoaman.2025.107857.

[7] O. Korchenko, O. Korystin, V. Shulha, S. Kazmirchuk, S. Demediuk, S. Zybin, Sustainable development of smart regions via cybersecurity of national infrastructure: A fuzzy risk assessment approach, Sustainability. 17(19) (2025) 8757. https://doi.org/10.3390/su17198757.

[8] A. Brezavšček, A. Baggia, Recent trends in information and cyber security maturity assessment: A systematic literature review, Systems. 13(1) (2025) 52. https://doi.org/10.3390/systems13010052.

[9] Y. Hong, M.M. Shafiee, M. Warkentin, The role of life satisfaction in cybersecurity awareness: A broaden-and-build perspective, Technology in Society. 85 (2025) 103206. https://doi.org/10.1016/j.techsoc.2025.103206.

[10] A. Kavak, Impact of information security awareness on information security compliance of academic library staff in Türkiye, The Journal of Academic Librarianship. 50(5) (2024) 102937. https://doi.org/10.1016/ j.acalib.2024.102937.

[11] J. K. Nwankpa, P. M. Datta, Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers, Computers & Security. 130 (2023) 103266. https://doi.org/10.1016/j.cose.2023.103266.

[12] M. Domínguez-Dorado, F.J. Rodríguez-Pérez, J. Carmona-Murillo, D. Cortés-Polo, J. Calle-Cancho, Boosting holistic cybersecurity awareness with outsourced wide-scope CyberSOC: A generalization from a Spanish public organization study, Information. 14(11) (2023) 586. https://doi.org/10.3390/info14110586.

[13] S. Lyeonov, W. Strielkowski, V. Koibichuk, S. Drozd, Impact of internet and mobile communication on cyber resilience: A multivariate adaptive regression spline modeling approach, International Journal of Critical Infrastructure Protection. 47 (2024) 100722. https://doi.org/10.1016/j.ijcip.2024.100722.

[14] J. Prümmer, T. van Steen, B. van den Berg, A systematic review of current cybersecurity training methods, Computers & Security. 136 (2024) 103585. https://doi.org/10.1016/j.cose.2023.103585.

[15] A. Mulahuwaish, B. Qolomany, K. Gyorick, J.B. Abdo, M. Aledhari, J. Qadir, K. Carley, A survey of social cybersecurity: Techniques for attack detection, evaluations, challenges, and prospects, Computers in Human Behavior Reports. (2025) 100668. https://doi.org/10.1016/j.chbr.2025.100668.

[16] M. Houichi, F. Jaidi, A. Bouhoula, Enhancing smart city security: An intrusion detection system using machine learning methods with the UNB CIC IoT 2023 dataset, IET Smart Cities. (2025) e70014. https://doi.org/10.1049/smc2.70014.

[17] W.J. Obidallah et al., A unified computational model for assessing security risks in Internet of Transportation Things-based healthcare applications, Electronics. 14(24) (2025) 4894. https://doi.org/10.3390/electronics 14244894.

[18] F. Merola, C. Bernardeschi, G. Lami, A risk assessment framework based on fuzzy logic for automotive systems, Safety. 10(2) (2024) 41. https://doi.org/10.3390/safety10020041.

[19] R. Acheampong, D.-M. Popovici, T.C. Balan, A. Rekeraho, I.-A. Oprea, A cybersecurity risk assessment for enhanced security in virtual reality, Information. 16(6) (2025) 430. https://doi.org/10.3390/info16060430.

[20] N.A. Chandra, A.A.P. Ratna, K. Ramli, Development and simulation of cyberdisaster situation awareness models, Sustainability. 14(3) (2022) 1133. https://doi.org/10.3390/su14031133.

[21] A. Aktayeva, Y. Makatov, A.K. Tulegenovna, A. Dautov, R. Niyazova, M. Zhamankarin, S. Khan, Cybersecurity risk assessments within critical infrastructure social networks, Data. 8(10) (2023) 156. https://doi.org/10.3390/data8100156.

[22] M.Z. Hanif, N. Yaqoob, Prioritized decision support system for cybersecurity selection based on extended symmetrical linear Diophantine fuzzy Hamacher aggregation operators, Symmetry. 17(1) (2025) 70. https://doi.org/10.3390/sym17010070.

[23] Z. Ali, M.-S. Yang, Improving risk assessment model for cyber security using robust aggregation operators for bipolar complex fuzzy soft inference systems, Mathematics. 12(4) (2024) 582. https://doi.org/ 10.3390/math12040582.

[24] E. Krzysztoń, D. Mikołajewski, P. Prokopowicz, Review of fuzzy methods application in IIoT security-Challenges and perspectives, Electronics. 14(17) (2025) 3475. https://doi.org/10.3390/electronics14173475.

[25] F.J. Gallardo-Amores, C. Del-Real, A.M. Díaz-Fernández, Assessing urban security and safety smartness: A systematic review of key performance indicators, IET Smart Cities. (2025) e70000. https://doi.org/ 10.1049/smc2.70000.

[26] J. Lund-Tønnesen, K. Fossheim, Excessive digital surveillance and data privacy invasion as a creeping crisis, Risk, Hazards & Crisis in Public Policy. 16 (2025) e70005. https://doi.org/10.1002/rhc3.70005.

[27] V. Grechaninov, Method of strategic planning of cybersecurity measures based on the SWOT concept, Cybersecurity: Education, Science, Technique. 2(30) (2025) 66–88. https://doi.org/10.28925/2663-4023.2025.30.953.

[28] D. Palko, L. Myrutenko, Method of comprehensive cybersecurity risks assessment in distributed information systems, Cybersecurity: Education, Science, Technique. 2(26) (2024) 487–502. https://doi.org/10.28925/ 2663-4023.2024.26.731.

[29] X. Wang, Z. Zhou, Security situation awareness algorithm of network information transmission based on big data, Scientific Reports. 15 (2025) 39058. https://doi.org/10.1038/s41598-025-24204-3.

[30] H.D. Mohammadian, O. Alijani, M.R. Moghadam et al., Navigating the future by fuzzy AHP method: Enhancing global tech-sustainable governance, digital resilience, and cybersecurity via the SME 5.0, 7PS framework and the X.0 wave/age theory in the digital age, AIMS Geosciences. 10(2) (2024) 371–398. https://doi.org/10.3934/geosci.2024020.

[31] Polishchuk V., Sehlianyk V. Data from 315 respondents to assess the level of cognitive and operational readiness of citizens of the region to ensure their own digital security (Ukraine) [Data set]. Zenodo, 2026. Available at: https://doi.org/10.5281/zenodo.19692560.