ISSN 1814-4225 (print)
Radioelectronic and Computer Systems, 2026, no. 1(117) ISSN 2663-2012 (online)

UDC 004.056:004.9+656.7:371.3 **doi: 10.32620/reks.2026.1.17**

Kayrat KOSHEKOV[1], Almat SAKHOV[1], Nataliia LEVCHENKO[2], Abay KOSHEKOV[1]

[1] ***Civil Aviation Academy, Republic of Kazakhstan***
[2] ***Technical University of Berlin, Germany***

HYBRID MODEL FOR ASSESSING COMPETENCIES OF CYBERSECURITY SERVICE STAFF OF CIVIL AVIATION ENTERPRISES USING GAMIFICATION AND FUZZY LOGIC ELEMENTS

*The **article focuses on improving** cybersecurity in civil aviation by introducing a hybrid model that assesses cybersecurity service employees' competencies through gamification and fuzzy logic. The **goal** of this study is to develop a hybrid model for assessing personnel competencies in the cyber and information security services of civil aviation enterprises. The **tasks** to be solved are: to analyze the problem of aging knowledge and competencies of specialists; to develop a hybrid model for assessing competencies; to justify the model's feasibility through experimental testing at an airline; and to propose a taxonomy for assessing and certifying personnel. The **following methods were used**: fuzzy logic with linguistic variables and membership functions; gamification with interactive scenarios simulating cyber incidents; modeling using defuzzification rules and procedures; and experimental testing at an airline. The following **results** were obtained: the experiment conducted at airlines in the Republic of Kazakhstan proved the feasibility of this approach. Gamified scenarios simulating real cyber incidents allow you to interactively assess the current level of personnel competency without risk to real systems. Artificial intelligence provides deep data analysis, identifies individual and systemic knowledge gaps, and offers personalized learning paths. This testing technology not only allows accurate measurement of personnel's skills and competencies but also enables timely measures to improve their qualifications. The study substantiated the need to develop a taxonomy for building a portfolio of personnel skills and competencies in aviation enterprises' cybersecurity services. Such a taxonomy will serve as the basis for establishing standardized norms and criteria for assessing personnel's skills and competencies, enabling objective assessment and certification of cybersecurity specialists. In addition, its use will allow for the timely identification of the need for advanced personnel training, which is critically important in the context of an intensively changing cyber landscape. **Conclusions**. The scientific novelty of the results obtained is as follows: 1) a hybrid model for assessing the competencies of cybersecurity specialists in aviation enterprises has been developed, integrated with fuzzy logic and gamification elements, which ensures a realistic assessment of skills in a dynamic cyberspace; 2) a methodology for forming a taxonomy of skills and competencies has been substantiated, which will become the basis for forming standardized norms and criteria for assessment (certification); 3) the model's effectiveness in identifying knowledge gaps and making it possible to form high-quality training trajectories for specialists has been confirmed by experimental testing of the model at an aviation enterprise.*

Keywords: *cyber resilience; cyber prevention; cyber immunity; cyberspace; cyber landscape; gamification; artificial intelligence; taxonomies for building a portfolio of competencies.*

1. Introduction

A steady, long-term growth in air traffic is predicted under current conditions of civil aviation development, accompanied by intensive digitalization and increasing operational complexity. The rapid pace of technological progress is changing the way civil aviation operates, making it more vulnerable to cyber threats. Malicious cyber activities can affect civil aviation in various ways, ranging from minor failures to disruptions in operational processes to catastrophic events. These risks are rapidly increasing, and a sustainable mechanism is urgently needed to ensure the cybersecurity of aviation enterprises [1].

In 2024, the world witnessed the largest IT outage in history, disrupting airlines, broadcasters, and other companies worldwide and resulting in losses of nearly US$ 5 billion. By 2025, cyber threats will continue to grow. 72% of respondents to the Global Cybersecurity Outlook survey noted an increase in cyber risks and cybercrime, the complexity of which was significantly increased by attackers' use of AI-generating technologies [2].

1.1. Motivation

However, this is not the only factor contributing to the growing complexity of the cyber landscape. Other factors include escalating geopolitical tensions, which

create uncertainty; increased integration and dependence on more complex supply chains, which leads to an opaque and unpredictable risk picture; the rapid emergence of new technologies, which is accompanied by the emergence of new vulnerabilities; the proliferation and fragmentation of cybersecurity regulation by international organizations; and other factors, which are shown in Fig. 1.

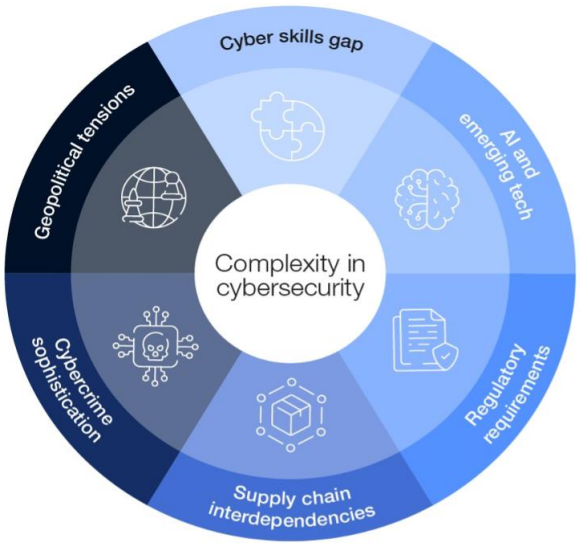

Fig. 1. Factors that exacerbate the complexity nature of cybersecurity [2]

According to the GCO survey, nearly 60% of organizations said that geopolitical tensions have impacted their cybersecurity strategy and risk perception, with one in three CIS leaders citing cyber espionage and the loss of confidential information/intellectual property theft as their top concerns. Thirty-seven percent of GCOs are concerned about GenAI's rapid adoption, which, by expanding cybercriminal capabilities, enables new, more sophisticated vulnerabilities and scalable cyberattacks. Seventy-six percent of CIS leaders said that cybersecurity regulations' fragmentation across jurisdictions seriously impacts their organizations' ability to meet cyber hygiene requirements [2].

This indicates that the complexity of the civil aviation cyber landscape only increases with each passing year. Statistics on cybersecurity incidents show that a significant portion of successful cyberattacks begin with employee errors or ignorance. Unintentional personnel actions, such as opening malicious attachments or using weak passwords, can have catastrophic consequences. In particular, in civil aviation, this can lead to leaks in confidential passenger data, disruptions in operations, and, most critically, a threat to flight safety because air traffic control, logistics, and passenger service are completely dependent on the stability and security of information technology. This technological dependence has made the industry particularly vulnerable to constantly evolving cyber threats [3]. Incidents involving data compromise, disruptions to key systems, and potential interference with flight control systems have become serious problems that pose a direct threat to flight safety.

Despite significant investments in technical protection measures, numerous studies and real incidents confirm that human factors remain the primary source of vulnerabilities in cybersecurity systems [2]. Insufficient awareness, lack of practical skills, and disregard for security rules among personnel, from senior management to line employees, create a "weak link" that is successfully exploited by attackers. Moreover, in a rapidly changing cyberspace, where threats are becoming increasingly sophisticated, these instructions are no longer sufficient [2].

In light of the growing complexity of the cyber landscape and the tightening of regulatory requirements, such as GDPR and industry standards, the development of cybersecurity competencies among civil aviation personnel is evolving from a recommended measure to a critical task. This problem requires a comprehensive solution that goes beyond traditional briefings and includes systemic training to develop practical skills and foster a culture of cyber awareness among aviation personnel [4].

In this regard, the development of cybersecurity competencies among civil aviation personnel has become a key element of airlines' cyber protection. This is no longer just a matter of observing cyber hygiene rules but a fundamental condition for ensuring flight safety. Therefore, a corporate cybersecurity training system should cover all airline employees, from top management to line personnel, and provide not only knowledge about existing threats but also practical skills for their timely recognition and neutralization [5].

Aviation enterprises should pay special attention to the competencies of CIS service personnel, because the aging of knowledge leads to gaps in competencies and, as a result, to a decrease in the effectiveness of cybersecurity in light of the rapid development of technologies. However, to understand which measures are essential to improve the level of personnel competencies, a clear idea of the individual portfolio of competencies of each employee and its compliance with the cybersecurity requirements of aviation enterprises is necessary. The formation of such a portfolio is possible through the systematic testing of personnel using AI and gamification technologies for interface interaction. Existing traditional approaches based on formal tests and theoretical courses cannot provide a realistic assessment of employees' skills and competencies. Gamification offers a fundamentally different approach that not only makes the testing process less stressful but also obtains deeper and more objective data on personnel's behavior and reaction to cyber threats. Interactive simulations, game scenarios, and achievement systems allow one to model real situations and assess

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

employees' readiness to solve them, while forming the necessary culture of cyber awareness. This study aims to substantiate this hypothesis.

1.2. State of the art

The aviation industry faces significant physical and cyber threats, highlighting the urgent need for enhanced cybersecurity measures despite increasingly sophisticated cyberattacks [3]. The introduction of modern information and communication technologies, on the one hand, increases the efficiency of civil aviation and, on the other hand, creates new vulnerabilities and potential threats. Existing solutions do not meet the specifics of civil aviation and modern cybersecurity requirements [6]; therefore, scientific publications are increasingly discussing issues of ensuring the cybersecurity of aviation enterprises. In particular, Władysław Leśnikowski [7] emphasized that civil aviation is a specific user of high-tech information technologies and, therefore, requires special protection against cyber threats. This protection should cover the entire aviation ecosystem, including air traffic control, aircraft, and airports. Morshedi and Matinkhan [8] analyzed recent cyber incidents and cyberattacks, focusing on emerging threats at airports. Researchers emphasize that the rapidly growing integration of UAVs into critical infrastructure, combined with their reliance on wireless communications, global positioning systems, and embedded control systems, significantly widens the surface area for cyberattacks. The authors focused on spoofing, jamming, interception, malware injection, and denial of service attacks. They also discussed new directions of cyber defense, providing for the integration of blockchains and quantum-resistant cryptographic frameworks designed to inspire the creation of reliable and adaptive UAV flight safety architectures [8], which certainly requires cyber security specialists to have the necessary skills and competencies.

In this regard, the ICAO's measures to regulate the training and retraining of aviation cybersecurity specialists are complex and comprehensive. They include developing standards and recommended practices, procedures, and methodological materials, and ensuring the adequacy of international air law to counter cyberattacks on civil aviation [9]. A striking example of this is the development of several guidelines for cybersecurity service specialists to acquire the necessary competencies, in accordance with the Aviation Cybersecurity Strategy [10] and paragraph CyAP 7.1 of the Cybersecurity Action Plan [11]. In particular, the ICAO TRAINING EVALUATION REPORT guide provides for testing the effectiveness of cybersecurity service personnel training and retraining [12]. The guide "Cybersecurity Culture in Civil Aviation" provides recommendations for promoting a cybersecurity culture in civil aviation [13]. The Cybersecurity Policy Guidance considers the protection and resilience issues of the critical infrastructure of international civil aviation against cyber threats [14]. Cyber Information Sharing provides recommendations for states and industry stakeholders on developing and implementing a cyber information-sharing plan, including guidance on identifying policies, resources, and practical steps to implement and continuously improve sharing practices [15].

The availability of the necessary skills and competencies among civil aviation cybersecurity specialists has also been actively explored in academic research. Researchers have noted not only a shortage of cybersecurity specialists but also the rapid aging of their knowledge and skills in the face of a dynamically changing cyber threat landscape, significantly complicating the task of ensuring sustainable cybersecurity for aviation enterprises. Bendler and Felderer [16] emphasized that creating a competency model aimed at providing a holistic view of the competencies required by cybersecurity specialists can eliminate the existing shortage of highly qualified cybersecurity specialists. The authors emphasize that the list of competencies specified in the Cybersecurity Body of Knowledge is incomplete. In addition, many of them exclude social, personal, and methodological competencies, reducing the profile of cybersecurity specialists' competencies to only professional competencies [16].

Training employees on safe online behavior and security measures remains a cornerstone of cybersecurity business strategies. Therefore, investing in employee cybersecurity training is one way to improve an enterprise's cyber resilience [17], as it helps employees acquire cybersecurity skills and competencies [18]. However, He et al. argued that the success of such investments largely depends on employee training methods [19].

According to the results of an in-depth ICAO Weighted Impact Index (WIN Index) study on how different cybersecurity training methods impact employee perceptions of the seriousness of cyber hygiene [20], Marshall et al. [21] substantiated that training materials based on actual malware report data and the use of innovative technologies in the training process are more effective in influencing employees' intention to follow recommended cybersecurity measures [19]. Gamification technologies using AI transform and enrich the educational process, activating learners' engagement and motivation to learn [22].

In symbiosis with technologies such as AI, content generation, automated assessment, and automated management, gamification has inexhaustible potential to create [23], more engaging [24], personalized [25], and effective learning environments [26]. Therefore, the issue of its application in assessing the competencies of civil aviation CIS personnel is becoming increasingly

relevant, especially with the launch of the World Economic Forum Initiative (Bridging the Cyber Skills Gap) within the framework of the Global Digital Compact adopted by the General Assembly as an annex to the Pact for the Future [27].

1.3. Objectives and approach

This study aims to develop and experimentally validate a hybrid model for assessing the cybersecurity and information security competencies of civil aviation information security personnel using gamification and fuzzy logic, represented as competency levels, a gamification score, and an integrated score.

To achieve this goal, within the framework of this publication, it is necessary to solve the following **tasks**: analyze the problem of aging knowledge and competencies of specialists; develop a hybrid model for assessing competencies; justify the possibility of using the model through experimental testing at an airline; and propose a taxonomy for the formation of a minimum set of skills and competencies for assessing and certifying personnel.

The article is structured as follows:

Section 2 describes the research materials and methods.

Section 3 presents the results and discussion: a hybrid model for assessing the competencies of cybersecurity personnel. Experimental testing was conducted at Petropavl International Airport. The model provides integral competency profiles and personalized recommendations.

Section 4 presents the conclusions and recommendations for the practical application of the hybrid model for competency assessment.

2. Materials and methods of research

his study developed a competency assessment model that combines fuzzy logic and gamified interface interaction tools for aviation cybersecurity professionals. The methodology is based on the assumption that accurately measuring many key competencies in a clear numerical form is difficult. Therefore, the use of fuzzy sets and linguistic variables that reflect real uncertainty in expert judgments or testing results is recommended.

Each of the selected competencies, for example, knowledge of industry standards, cyber incident response skills, and ability to work with SIEM systems, is described using Low, Medium, and High linguistic variables, respectively. A corresponding membership function was constructed for each linguistic category, allowing the normalized assessment to be interpreted as a fuzzy profile. Rules are activated in the knowledge base based on the membership degree values.

The model's rule base is constructed as a set of production structures. The full production base includes rules that cover all possible combinations of the three competencies, with three linguistic assessments for each. In addition, partial rules with two conditions were included, allowing the model to adapt to situations of incomplete information or to prioritize competencies.

The rules were activated based on the principle of minimum degree of membership among the input conditions, after which the aggregated output was formed. The defuzzification procedure used the center of gravity method to obtain the final conclusion, which enabled an integrated assessment of the level of competence of the security service personnel of one of the airlines in the Republic of Kazakhstan. The defuzzification results were compared with the reference intervals for each level.

In the final stage, the model was integrated with a visual gamified interface that displayed the user's level, accumulated experience (XP), activated rules, achievements, and personalized recommendations. This approach combines analytical accuracy with an intuitive understanding of results, increasing personnel efficiency and motivation during training or certification.

3. Results

According to the International Air Transport Association [28], the number of cyber-attacks in the aviation industry is constantly increasing. By 2025, the economic damage to businesses from cybercrime is predicted to reach US$10.5 trillion [29]. Using innovative technologies such as cloud computing, big data, artificial intelligence (AI), the Internet of Things (IoT), machine learning (ML), blockchain techniques, virtual reality (VR), augmented reality (AR), digital twins (DT), and metaverse, attackers are creating increasingly sophisticated cyber threats [30]. For example, in July 2024, Airport and Aviation Services Sri Lanka (AASL) suffered a major data breach that exposed more than 7,000 records, including names, national identification numbers, and passport details. This incident highlights the ongoing threat posed by cybercriminals targeting sensitive aviation infrastructure [31]. The 2024 hack of AerCap, a major aircraft leasing company, also involves hackers accessing sensitive data. These examples highlight the potential for disruption, financial loss, and reduced passenger safety caused by cyberattacks [31].

Cyber threats can be partially avoided with sufficient cybersecurity specialists. However, despite the fact that their number increased by 12.6% in 2023, the global shortage of such specialists still amounted to almost 4 million, indicating the alarming scale of the problem [32]. From a regional point of view, the shortage of cybersecurity specialists is most pronounced in Asia, where

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

there is a shortage of more than 2.5 million specialists. This is followed by North America, China, India, Brazil, and other countries Thus, competent cybersecurity specialists represent an indispensable cyber shield for airlines in the context of constantly growing cyber threats and expanding attack surfaces [33] [34].

The reasons for the cybersecurity talent shortage vary, ranging from the rapidly evolving cybersecurity landscape to aging knowledge, resulting not only in a shortage of cybersecurity professionals but also in a skills and competency gap [35]. For example, recent graduates may have the necessary skills but lack real-world experience. However, experienced professionals may experience skill shortages due to their aging knowledge. Finally, qualified professionals with the necessary skills and experience tend to command higher salaries, and organizations may find themselves in a labor shortage simply because they cannot afford to hire the talent they need [36]. The variety of reasons for the cybersecurity talent shortage leads to uncertainty about the exact type of shortage the industry is facing, which consequently complicates decision-making on cyber hygiene and increases airlines' cyber vulnerability. In this regard, there is an increasing need for a systematic assessment of the skills and competencies of personnel responsible for ensuring cybersecurity to identify knowledge gaps and promptly adjust advanced training programs.

However, assessing employees' competencies in aviation cybersecurity is a complex task that requires considering not only knowledge but also practical skills, adaptability, stress resistance, and the ability to respond to incidents in real time. As noted in previous studies [37, 38], traditional methods based on strict tests or linear scales often do not reflect the full picture of the employee's real capabilities [39]. In this context, a hybrid model that combines the elements of gamification and fuzzy logic is proposed for assessing the competencies of aviation personnel. Gamification stimulates motivation, growth, and engagement through XP points and levels. Furthermore, fuzzy logic allows you to avoid rigid frameworks, assessing the level of skill proficiency according to fuzzy sets, for example, as "low," "medium" or "high" level. An experiment was conducted at the international airport in Petropavlovsk to verify the feasibility of using a hybrid model to assess the competencies of aviation personnel, combining elements of gamification and fuzzy logic.

The mathematical model structure for assessing competencies:

1) Competency space. Let us assume that to ensure cybersecurity in an airline, there is an information security service with the number of employees $E = \{e_1, e_2, \ldots, e_m\}$, each of whom must be assessed according to the set of competencies $C = \{c_1, c_2, \ldots, c_n\}$. For each employee e_i, the competency assessment vector is determined as follows:

$$K_i = [k_{i1}, k_{i2}, \ldots, k_{in}] \in [0,1]^n, \quad (1)$$

where k_{ij} is level of proficiency in competence C_j by employee e_i in normalized form.

2) Membership functions (fuzzy logic). For each competence c_j, the assessment k_{ij} was interpreted using three linguistic variables: Low, Medium, High. These correspond to the membership functions. The membership function for the low:

$$\mu_{Low}(x) = \begin{cases} 1, & x \le a \\ \frac{b-x}{b-a}, & a < x \le b. \\ 0, & x > b \end{cases} \quad (2)$$

The membership function for the medium:

$$\mu_{Medium}(x) = \begin{cases} 0, & x \le a \text{ or } x \ge d \\ \frac{x-a}{b-a}, & a < x < b \\ 1, & b < x \le c \\ \frac{d-x}{d-c}, & c < x < d \end{cases}. \quad (3)$$

The membership function for the high:

$$\mu_{High}(x) = \begin{cases} 0, & x \le c \\ \frac{x-c}{d-c}, & c < x \le d. \\ 1, & x > d \end{cases} \quad (4)$$

Typical parameters: a= 0.2, b=0.4, c=0.6, d=0.8. The graphs of membership functions for three linguistic variables: low, medium, and high, which interpret the assessment of competence k_{ij} for each competence c_{ij}, are presented in Fig. 2.

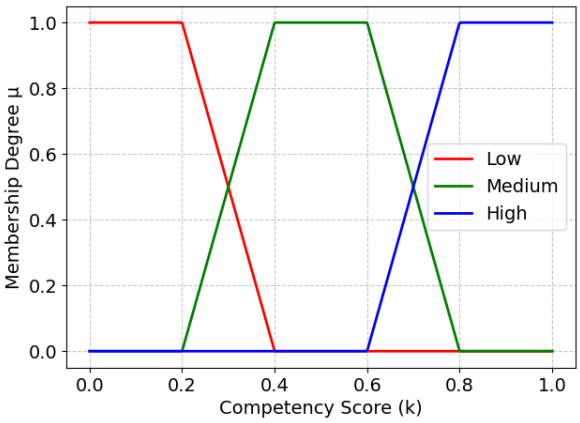

Fig. 2. Reliability functions for assessing linguistic competency

3) Fuzzy Rules. During the research, the following rules were formulated:

$$\text{If } c_1 \text{ is High and } c_2 \text{ is Medium then Competence Level is Advanced.} \quad (5)$$

The set of such rules was designated as $R = \{r_1, r_2, \ldots, r_p\}$. Each rule r_k had the following form:

$$r_k: \text{IF } \wedge_{j \in J_k}(c_j \text{ is } L_{jk}) \Longrightarrow \text{Level} = L_k^*, \quad (6)$$

where:

$$L_{jk} \in \{\text{Low}, \text{Medium}, \text{High}\}. \quad (7)$$

$$L_k^* \in \begin{Bmatrix}\text{Beginner, Intermediate,}\\ \text{Advanced, Expert}\end{Bmatrix}. \quad (8)$$

4) Rule aggregation and dephasing. After evaluation according to all rules, the vector belonging to the competence level is determined as follows:

$$\mu_i^* = \left[\mu_{\text{Beginner}}^{(i)}, \mu_{\text{Intermediate}}^{(i)}, \mu_{\text{Advanced}}^{(i)}, \mu_{\text{Expert}}^{(i)}\right]. \quad (9)$$

This vector reflects how each possible competence level corresponds to the current results. This approach allows us to obtain a more accurate and realistic assessment, which subsequently serves as a fundamental basis for forming a portfolio of competencies for each airport information security service employee. The centroid method was used to obtain a numerical assessment of competencies based on the membership vector. Mathematically, this is expressed as finding a weighted average value, where the "weight" is the degree of membership:

$$S_i = \frac{\sum_{k=1}^{4} \mu_k^{(i)} \cdot v_k}{\sum_{k=1}^{4} \mu_k^{(i)}}, \quad (10)$$

where v_k is a numeric value corresponding to the linguistic level (for example: Beginner [0.00-0.45], Intermediate [0.45-0.65), Advanced [0.65-0.85], Expert [0.85-1.00]).

5) Gamification system. In addition to competency assessment, each employee earned the following game points (experience points, XP) for completing the tasks assigned to them:

$$XP_i = \sum_{t=1}^{T} \delta_{it} w_t, \quad (11)$$

where: $\delta_{it} \in \{0\ 0{,}1\}$ - fact of participation in activity t, w_t - activity weight (for example: training – 50, CTF – 100, incident simulation – 150). Thus, the employee's competency level (Level_i):

$$\text{Level}_i = \left\lfloor \frac{XP_i}{\theta} \right\rfloor + 1, \quad (12)$$

where θ - the amount of XP_i required to move to a new level.

6) Final rating. The final integrated assessment of each employee's level of competence was carried out along with technical competence and motivational results as follows:

$$R_i = \alpha \cdot S_i + (1 - \alpha) \cdot \frac{XP_i}{XP_{max}}, \quad (13)$$

where $\alpha[0,1]$ is weighting factor (e.g. 0.7 in favor of technical assessment).

Let us consider the feasibility of using the proposed approach based on the competency assessment results of one of the employees of the information security service of the international airport in Petropavlovsk, which was carried out during this experiment. Competencies were assessed according to three key criteria: c_1 - knowledge of international standards of cybersecurity in civil aviation (ICAO, EASA, NIST), c_2 - skills in responding to cyber incidents in real time and c_3 - practical skills in working with security monitoring systems (SIEM/IDS). After passing practical and theoretical testing tasks using gamification and fuzzy logic, it was established that airport information security service employees have the following normalized competency levels:

$$c_1 = 0.65, c_2 = 0.80, c_3 = 0.50. \quad (14)$$

These values are subject to fuzzification. In other words, they are transformed into degrees of membership in the linguistic variables Low, Medium, and High. In particular, at c_1 = 0.6565, partial membership in the Medium and High is observed, with corresponding values of μ previously determined using membership functions and presented in Table 1.

Table 1

Fuzzification of competencies of employees of the information security service of the international airport of Petropavlovsk

Competence level	Value (normalized)	μ_{Low}	μ_{Medium}	μ_{High}
c_1	0.65	0	0.75	0.25
c_2	0.80	0	0	1
c_3	0.50	0	1	0

The next step is to activate the rules from the fuzzy production base. The two rules were activated in this case. Rule 1:

$$\text{If } c_1 \text{ is High and } c_2 \text{ is High then Level} = \text{Expert} \longrightarrow \longrightarrow \mu = \min(0.25, 1) = 0.25 \Longrightarrow \text{Expert}. \quad (15)$$

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Rule 2:

$$\text{If} c_1 \text{ is Medium and } c_2 \text{ is High and } c_3 \text{ is Medium}$$
$$\text{then Level} = \text{Advance} \rightarrow \mu =$$
$$= \min(0.75, 1, 1) = 0.75 \Rightarrow \text{Advanced}. \quad (16)$$

The other base rules that did not match the input conditions remained inactive. A fuzzy output was generated according to the set of activated rules, which presented all possible competence levels (Beginner, Intermediate, Advanced, Expert), together with the corresponding μ values. A complete rule base was generated (Table 2) to illustrate the logic of the fuzzy model, which covered all possible combinations of linguistic assessments of three key competencies (c_1, c_2, c_3), which form the full production space. This approach demonstrates the system's flexibility and scalability. When expanding the number of competencies, the rule base can be automatically supplemented with new combinations, allowing the model to be adapted to any professional cybersecurity profile.

Table 2

Unified fuzzy rule base for competency assessment (full and partial rules)

c_1	c_2	c_3	Competency Level
Low	Low	Low	Beginner
Low	Low	Medium	Beginner
Low	Low	High	Beginner
…	…	…	…
Medium	Medium	Medium	Intermediate
Medium	Medium	High	Intermediate
Medium	High	Low	Beginner
High	Low	Low	Beginner
High	Low	Medium	Beginner
High	Medium	High	Advanced
High	High	Low	Advanced
…	…	…	…
Low	Low	-	Beginner
Low	Medium	-	Beginner
Low	High	-	Beginner
…	…	…	…
Low	-	High	Beginner
Medium	-	Low	Beginner
Medium	-	Medium	Intermediate
-	Medium	Low	Beginner
-	Medium	Medium	Intermediate
…	…	…	…

The model supports partial (reduced) rules based on one or two competencies in addition to the full rule base. This allows the model to respond flexibly to high critical parameter values even in the absence of complete information. Both full (three-component) and partial (two-component) rules were applied when assessing this employee's competency level, enabling a more accurate assessment of their strengths. The final competency level of the information security employees was determined by defuzzification as follows:

$$S = \frac{(0.75 \cdot 0.75)(0.25 \cdot 1.00)}{0.75 + 0.25} = \frac{0.5625 + 0.25}{1.00} = 0.8125. \quad (17)$$

The calculation result presented in (17) corresponds to the advanced level. This approach allows the activation strength of each rule and the degree of uncertainty in the source data to be considered, providing a flexible, context-sensitive assessment.

Gamification assessment. This employee participated in the following activities: theoretical testing (50 XP), training on attack modeling (100 XP), capture-the-flag simulation (150 XP), and knowledge of the SOP instruction (80 XP). The point assessment of his competencies was 380 XP. Level (12) at $\theta = 200$:

$$\text{Level} = \left\lfloor \frac{380}{200} \right\rfloor + 1 = 1 + 1 = 2. \quad (18)$$

Integral assessment. Assume that the weighting coefficient $\alpha = 0.7$ (i.e., the main focus is on professional competencies) and that the maximum XP among all employees is 600.

$$R = 0.7 \cdot 0.8125 + 0.3 \cdot \frac{380}{600} = 0.7 \cdot 0.8125 +$$
$$+ 0.3 \cdot 0.6333 = 0.75875. \quad (19)$$

The results of the assessment of the level of competence of the employee of the information security service of the international airport of Petropavlovsk showed that this employee has a high level of skills and competences in most of the assessed parameters, activated the key rules of fuzzy logic, and reached the "Advanced" profile. His gamification level was Level 2, and the final integral assessment was 0.76 (out of 1.0), corresponding to a strong cybersecurity specialist ready for advanced tasks in aviation systems' cyber hygiene. Table 3 presents the obtained quantitative results of the pilot assessment, including the main parameters.

A visual two-component interface system was created to implement the competency assessment process, ensuring convenient user interaction with the model at all stages, from entering input data to obtaining final results. The first stage of interaction is the Competency Input & Evaluation Panel (Fig. 3), where the user sets the normalized values of the three key competencies using intuitive

sliders. After the evaluation button is activated, the system performs fuzzy logical inference, displaying the activated rules and defuzzied result.

The results were automatically transferred to the original module, Cybersecurity UI Mockup (Fig. 4), which visualizes the employee's level, amount of XP, activated achievements, and personalized recommendations. This interface structure allows for a clear separation the evaluation phase from the result interpretation phase, ensuring modularity, flexibility, and ease of use within the system's practical implementation framework.

Table 3

Quantitative indicators obtained during the hybrid competency model pilot testing

Indicator	Meaning	Value	Interpretation
Normalized competency c_1	Knowledge of standards	0.65	Medium/high boundary
Normalized competency c_2	Incident response	0.80	High
Normalized competency c_3	SIEM/IDS skills	0.50	Medium
Number of activated fuzzy rules	Model response	2	Sufficient for decision
Defuzzied competency level	Technical result	Advanced	High professional profile
Gamification score	Engagement/performance	380 XP	Passed assigned activities
Gamification level	Motivational result	Level 2	Medium progression
Final integrated score	Aggregate model output	0.76/1.00	Strong specialist profile

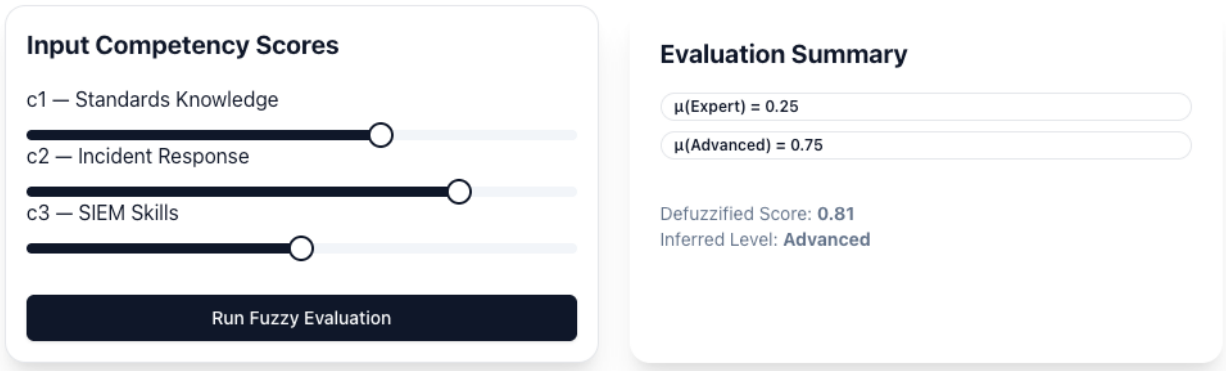

Fig. 3. Competency Input & Evaluation Panel: data entry and calculation of results

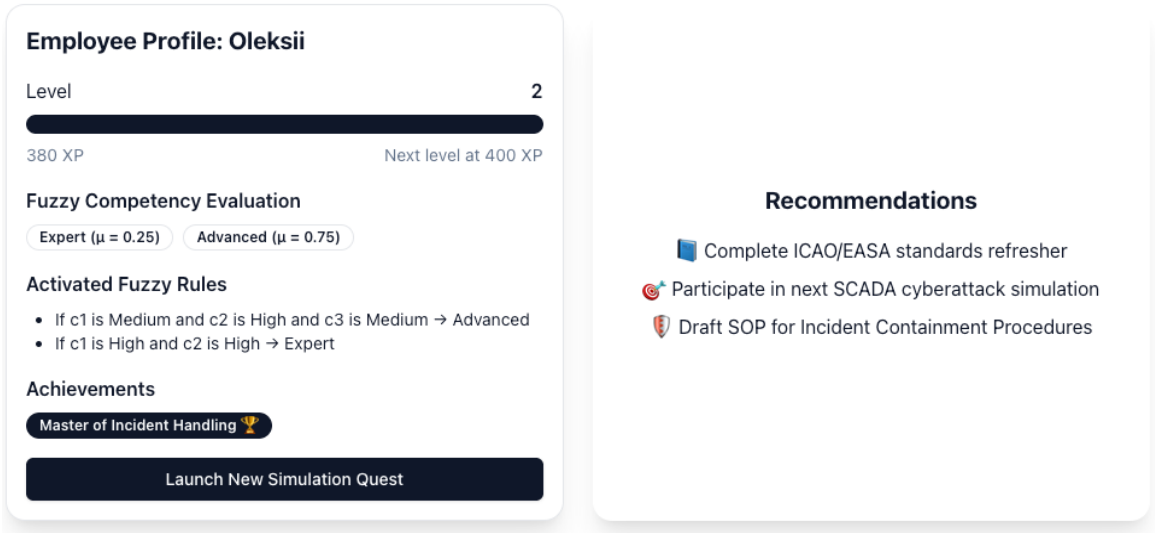

Fig. 4. Cybersecurity UI Mockup: Level, XP, Rules and Recommendations Output

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

4. Discussion

The proposed model for assessing the competence of airport information security specialists combines a formalized fuzzy logic approach with interactive, gamified visualization of results, ensuring objectivity in decision-making and high user engagement. By using linguistic variables, fuzzy rules, and defuzzification, the system can flexibly interpret the levels of personnel skills and competences, even with partial information, making the model suitable for use in civil aviation enterprises and ensuring their cyber resilience.

However, using this model is advisable only with a clear understanding of the target levels of cybersecurity personnel's skills and competencies. It is not sufficient to simply conduct testing. Understanding the level of knowledge and skills required of each specific employee is necessary. Moreover, given the high dynamics of threats, these requirements should be regularly reviewed and updated. Ignoring this aspect can lead to the assessment being based on outdated standards (which is exactly what is happening now), creating a false appearance of security and thereby increasing airlines' cyber vulnerability.

International standards, such as ISO/IEC 27001:2022 [40], are widely used to ensure information security. This standard serves as a universal basis for implementing information security management systems, ensuring methodological risk management and data protection. However, in the context of civil aviation, where cyber threats are systemic and transboundary, applying these standards within a single airline is insufficient. This thesis is supported not only by general observations but also by strategic documents, in particular the ICAO Cybersecurity Action Plan [1], which calls for a coordinated global response to cyber threats. Considering that identical risks affect the entire aviation ecosystem and taking into account the developed Global Taxonomy of Skills "Cybersecurity and Application Security" [41] (Table 4), a need to create a single, unified taxonomy for assessing the competencies of personnel in cybersecurity in civil aviation is evident.

Such a taxonomy will serve as a methodological basis for the formation of individual portfolios of competencies of each employee of the cyber and information security services, which will not only allow for an objective measurement of the current level of competencies but also ensure timely planning of advanced training programs and the construction of a personalized trajectory of professional development aimed at eliminating the identified skills and competencies gaps. However, achieving the desired result in the context of an actively changing cyber landscape is difficult. Therefore, it is advisable for the Civil Aviation Administration of the Republic of Kazakhstan, guided by the Global Taxonomy of Skills "Cybersecurity and Application Security" [42], to develop a standardized taxonomy for building a portfolio of skills and competencies of the personnel of the cyber and information security service of civil aviation, in close

Table 4

Global Taxonomy of Cybersecurity and Application Security Skills [35]

Skill name	Cybersecurity and application security		
Skill descriptor	Using technologies, processes and practices to protect computers, networks, programmes and data from unauthorized access or attacks that are aimed at exploitation.		
Skill descriptor by proficiency levels	Foundational	Experienced	Advanced
	Understands basic cybersecurity principles and common security threats – Can identify and follow basic cybersecurity practices; – Aware of fundamental security policies and compliance requirements	In-depth understanding of cybersecurity frameworks – Familiar with common network and application vulnerabilities – Proficient in using security tools – Ability to identify and mitigate security risks in applications, networks and systems	Expert knowledge of advanced cybersecurity techniques – Specializes in advanced application security practices – Expertise in cryptographic methods, identity and access management (IAM), and risk management frameworks – Deep understanding of compliance requirements and experience in implementing enterprise-level security strategies – Proficient in security automation and orchestration tools

cooperation with stakeholders, which should become a unified regulatory act that can be quickly adapted to the evolving cyberspace.

When developing the taxonomy, the ICAO recommends using two types of data necessary to understand the skill needs of cyber and information security personnel. In particular, human resources (HR) and learning and development (L&D) data, such as education, qualifications, professional cybersecurity certifications (e.g., CISSP, CISM, CompTIA Security+, and OSCP), self-assessment, and peer skills assessment.

However, in the context of the development of the Super Smart Society, or Society 5.0, where digital transformation is carried out through the human-cyber-physical approach [43, 44], the key elements are digital twins, artificial intelligence (AI), AI agents, and robotics [45]. The development of a taxonomy to build a portfolio of personnel skills and competencies in cybersecurity for civil aviation requires new approaches.

To achieve this goal, we developed and tested an algorithm to construct a taxonomy for the formation of a portfolio of skills and competencies for cyber and information security personnel, considering the specifics of civil aviation and Society 5.0 requirements. It consists of several interrelated stages, each of which uses data obtained by applying a hybrid model to assess the skills and competencies of air transport cybersecurity personnel (Fig. 5).

The first stage of developing a taxonomy of cybersecurity personnel skills and competencies should be the formation of a strategy for the development of talent and competencies of cyber and information security personnel at both the industry and airline levels, in accordance with the Strategic Cybersecurity Talent Framework [27]. The next stage should be an inventory of personnel skills and competencies, the results of which should become a fundamental basis for: verifying the level of qualification of cybersecurity personnel; conducting a comparative analysis of the compliance of the level of skills and competencies with international cybersecurity standards, the Global Taxonomy of Skills "Cybersecurity and Application Security" [42], the ICAO Cyber Defense Action Plan [1], as well as the Strategy for the Development of Talents and Competencies of Cyber and Information Security Personnel developed by both a specific Civil Aviation Administration and each airline. Such an approach will optimize cybersecurity talent and competency management, predicting skill needs and industry trends.

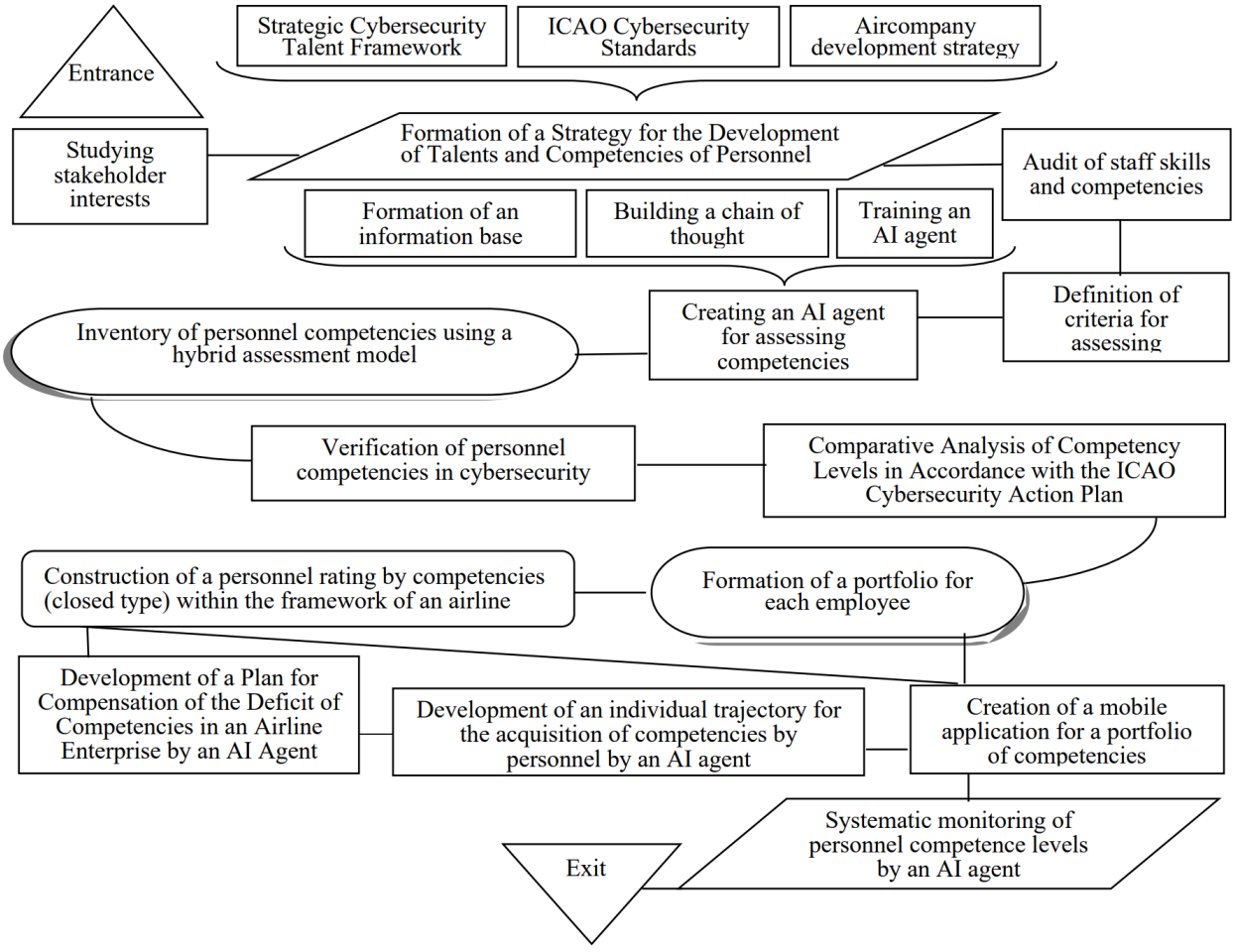

Fig. 5. Algorithm for constructing a taxonomy for forming a portfolio of skills and competencies of air transport cyber and information security service personnel

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Airlines can temporarily fill the cybersecurity skills gap by hiring foreign specialists. However, this approach only solves the problem for a short time, that is, it does not form a sustainable solution. Moreover, it entails several negative socioeconomic consequences:

- Loss of employment opportunities. Hiring foreign specialists displaces jobs that could be occupied by local residents, reducing the incentive to obtain specialized education and develop relevant competencies within the country;

- Demotivation and "knowledge aging" of the personnel of the cyber and information security service. Current employees lose motivation for continuous training because they see that their competencies are not valued and hiring from outside is preferred. As a result, their knowledge and skills gradually become obsolete, making them less in demand in dynamically changing cyberspace;

- Dependence on conditions and opportunities for attracting foreign specialists. The shortage of qualified personnel creates a reliance on foreign specialists, which can pose a critical risk in the event of geopolitical or economic changes;

- "Leakage" of financial resources. Funds that could be used to develop educational programs and improve the qualifications of cyber and information security personnel, as well as develop cybersecurity talent, are used to pay foreign cybersecurity specialists, which contradicts the Concept of Labor Market Development for 2024-2029, developed by the Ministry of Labor and Social Protection of the Population of the Republic of Kazakhstan in pursuit of the instructions of the Head of State, voiced in the Address to the People of Kazakhstan in September 2023 [46].

The next stage of the algorithm for constructing a taxonomy of personnel cybersecurity skills and competencies should be to monitor the frequency, complexity, and characteristics of cyber incidents and cyberattacks in civil aviation, and to establish the level of airlines' cyber vulnerability. The collected data will allow the construction of probabilistic scenarios for the near-term transformation of cyberspace and, accordingly, the development of programs to improve cybersecurity personnel's qualifications and certify skills and competencies. The proposed approach to developing a taxonomy for constructing a portfolio of skills and competencies for cyber security personnel will not only address the immediate need for highly qualified specialists but also strengthen airlines' competitive advantage, ensuring the readiness of cybersecurity and information security personnel to meet the new challenges of a dynamically changing cyberspace.

The increasingly complex cybersecurity landscape in civil aviation, as well as the rapid aging of knowledge, necessitates both specialists with high technical skills to navigate complex systems and networks and other specialists with non-technical skills such as risk management and emergency management. The World Economic Forum's Future of Jobs 2023 report [47] found that the inability to attract highly skilled cybersecurity professionals will be one of the most important barriers to industry transformation over the next five years. Several competency audit methodologies have been proposed to address this barrier and mitigate the negative impact of a lack of cybersecurity talent [48]. In particular, Sabillon [49] proposed a competency audit model (CSAM) based on a multi-case study of personnel competency compliance with standards and fuzzy logic methodology. Mizrak and Reyhan Akkartal [31] developed a method for assessing the cybersecurity of enterprises (including the cybersecurity competencies of personnel) using (DEMATEL) integrated with quantum spherical fuzzy sets (QSFS). An experiment conducted using this method showed that "compliance with the regulatory requirements" of personnel competencies is the most influential factor in enterprises' level of cyber vulnerability. Kolotusha et al. [50] substantiated the feasibility of a multicriteria assessment of the criteria for compliance of an air traffic controller simulator's information model with a real system.

Alothman [51] demonstrated the feasibility of developing an innovative platform for training and assessing cybersecurity personnel's competencies by combining fuzzy logic methods with a gamified interface, thereby ensuring both analytical accuracy and user involvement. Similar approaches have already been applied in the field of HR management and education; however, most existing solutions do not cover cybersecurity specifics.

Sahnouni and Benghebrid [52] proposed a fuzzy logic and artificial intelligence model for assessing company personnel to eliminate subjective bias. Although the model structure allows for greater objectivity in the assessment, it focuses on general organizational competencies and does not consider the dynamics of interface interactions or gamified elements.

In the study by Slavyanov and Dimov [53] the application of fuzzy logic for decision making after identifying cyber incidents was considered. Despite its thematic proximity to cyber security, the model focuses on supporting technical decisions rather than assessing human competencies or learning goals.

The model presented by Vargas et al. [54] also implements competency assessment through fuzzy logic in the context of higher education. Although this approach enables testing process automation, it lacks gamification and is less flexible when the full volume of input data is insufficient.

Thus, the proposed model stands out among existing solutions for combining three key elements: fuzzy

competency assessment, adaptation to incomplete information, and an interactive, gamified presentation of results, which is especially valuable in the context of aviation cybersecurity training or certification.

5. Conclusion

Thus, the study substantiated that, in the context of the exponential growth in the number and complexity of cyber threats to civil aviation, the "aging knowledge" of cybersecurity specialists is becoming a significant threat that can compromise flight safety, cause system failures, and result in serious financial losses.

Traditional methods of auditing the skills and competencies of cyber personnel and the information security service of aviation enterprises, as well as reactive training, no longer meet the requirements of dynamically changing cyberspace. A proactive approach to assessing the skills and competencies of cyber personnel and the information security services of aviation enterprises in the context of the development of the Super Smart Society (Society 5.0), where digital transformation is carried out within a human-cyber-physical framework, is not only desirable but also critically important.

The success of the proposed hybrid model for assessing the skills and competencies of cyber personnel and the information security service of civil aviation enterprises, using elements of gamification and fuzzy logic, has been demonstrated through a specific experiment conducted at aviation enterprises in the Republic of Kazakhstan. Unlike existing models, this model is based on a combination of three key elements: fuzzy assessment of competencies, adaptation to incomplete information, and an interactive, gamified presentation of results, which is especially valuable for the certification of civil aviation enterprise specialists in cyber and information security services. Gamified scenarios that simulate real cyber incidents create a safe, interactive environment for assessing employees' current skills and competencies. Simultaneously, AI analyzes the collected data to identify individual and systemic knowledge gaps, thereby enabling the creation of personalized learning paths. In turn, the use of fuzzy logic allows for the modeling and analysis of complex, ambiguous situations that specialists encounter in real practice. It also allows for the assessment of not only the correctness but also the degree of creativity, adequacy, and proactivity of their decisions, thereby identifying their ability to act quickly in non-standard situations, which makes the assessment of skills and competencies more accurate.

The assessment of the skills and competencies of the personnel of the cyber and information security service of airlines will be more realistic, provided that a standardized taxonomy of skills and competencies is created based on the Global Taxonomy of Skills "Cybersecurity and Application Security" developed by ICAO. It is emphasized that in the context of the development of Society 5.0, where digital transformation is carried out taking into account the human-cyber-physical approach, the formation of a taxonomy of cyber skills of civil aviation personnel requires new approaches because outdated methods of assessing skills and competencies do not provide a full assessment of competencies in the context of the development of highly intelligent and interconnected systems.

An algorithm for developing a taxonomy to build a portfolio of skills and competencies of personnel of aviation enterprises' cyber and information security services is proposed, which should become the basis for creating standardized norms and criteria for assessing personnel's skills and competencies. This will allow not only to conduct an objective assessment and certification of cybersecurity specialists but also to develop an individual trajectory for improving the qualifications and certification of skills and competencies for each cybersecurity employee, which will ultimately reduce the level of cyber vulnerability of civil aviation enterprises.

Contribution of authors: conceptualization, methodology – **Kayrat Koshekov, Almat Sakhov**; formulation of tasks, analysis – **Nataliia Levchenko**; development of model, software, verification – **Kayrat Koshekov, Abay Koshekov**; analysis of results - **Natalia Levchenko**, visualization – **Abay Koshekov, Almat Sakhov**; writing – original draft preparation – **Kayrat Koshekov**, **Almat Sakhov**; writing – review and editing – **Kayrat Koshekov**, **Abay Koshekov.**

Conflict of Interest

The authors declare that they have no conflict of interest related to this research, whether financial, personal, authorship, or otherwise, that could affect the study and its results presented in this paper.

Financing

This study was conducted without financial support.

Data Availability

Data will be made available upon reasonable request.

Use of Artificial Intelligence

The authors confirm that they did not use artificial intelligence methods while creating the presented work.

All the authors have read and agreed to the published version of this manuscript.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

References

1. *Cybersecurity Action Plan*. Available at: https://www.icao.int/cybersecurity-action-plan (accessed 13.09.2025).

2. *Global cybersecurity outlook 2025*. Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/ (accessed 13.09.2025).

3. Aslan, Ö., Aktuğ, S., Ozkan-Okay, M., Yilmaz, A., & Akin, E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, 2023, vol. 12, no. 6, art. no. 1333. DOI: 10.3390/electronics12061333.

4. Koshekov, K., Bakirov, B., Sakhov, A., Levchenko, N., Tanovitskiy, Y., Koshekov, A., Kurbanov, Y., & Togambayev, R. Cyber hygiene of the digital twin of the civil aviation occupational safety management system in the context of quantum transformation. *Radioelectronic and Computer Systems*, 2025, vol. 2025, no. 1, pp. 231–247. DOI: 10.32620/reks.2025.1.16.

5. Koshekov, K., Alibekkyzy, K., Toiganbayev, B., Belginova, S., Keribayeva, T., Tulaev, V., & Koshekov, A. Formalization of risk management in the context of digital business transformation. *Indonesian Journal of Electrical Engineering and Computer Science*, 2023, vol. 30, no. 3, pp. 1428-1439. DOI: 10.11591/ijeecs.v30.i3.pp1428-1439.

6. Kharchenko, V., Korchenko, O., & Gnatyuk, S. Bazova model formuvannia vymoh do zabezpechennia kiberbezpeky tsyvil′noyi aviatsiyi [Basic model for cybersecurity requirements definition in civil aviation]. *Ukrainian Scientific Journal of Information Security*, 2016, vol. 22, no. 2, pp. 150-155. DOI: 10.18372/2225-5036.22.10708. (In Ukrainian)

7. Leśnikowski, W. Threats from cyberspace for civil aviation. *Wiedza Obronna*, 2021, vol. 276, no. 3, pp. 124-153. DOI: 10.34752/2021-h276.

8. Morshedi, R., & Mojtaba Matinkhah, S. Cybersecurity Challenges and Solutions in Unmanned Aerial Vehicles (UAVs). *Journal of Field Robotics*, 2025. DOI: 10.1002/rob.70040.

9. *Aviation cybersecurity 2023*. Available at: https://www.icao.int/aviation-cybersecurity (accessed 09.10.2025).

10. *Aviation Cybersecurity Strategy: Security and Facilitation Strategic Objective.* Available at: https://www.icao.int/aviation-cybersecurity-strategy (accessed 09.10.2025).

11. *Cybersecurity Action Plan.* Available at: https://www2023.icao.int/aviationcybersecurity/Documents/CYBERSECURITY%20ACTION%20PLAN%20-%20Second%20edition.EN.pdf#search=ICAO%20TRAINING%20Report%20in%20cybersecurity%20professionals (accessed 09.10.2025).

12. *ICAO training evaluation report*. Available at: https://www2023.icao.int/training/Documents/ICAO%20Training%20Evaluation%20Report%202020.pdf#search=ICAO%20TRAINING%20Report (accessed 09.10.2025).

13. *Cybersecurity Culture in Civil Aviation*. Available at: https://www2023.icao.int/Security/Security-Culture/Documents/ICAO%20-%20Cybersecurity%20Culture%20in%20Civil%20Aviation_EN.pdf#search=ICAO%20TRAINING%20Report%20in%20cybersecurity%20professionals (accessed 09.10.2025).

14. *Cybersecurity Policy Guidance*. Available at: https://www.icao.int/sites/default/files/sp-files/aviationcybersecurity/Documents/Cybersecurity%20Policy%20Guidance.EN.pdf (accessed 09.10.2025).

15. *Cyber Information Sharing*. Available at: https://www.icao.int/sites/default/files/sp-files/aviationcybersecurity/Documents/Cyber%20Information%20Sharing.EN.pdf (accessed 09.10.2025).

16. Bendler, D., & Felderer, M. Competency Models for Information Security and Cybersecurity Professionals: Analysis of Existing Work and a New Model. *ACM Transactions on Computing Education*, 2023, vol. 23, no. 2, pp. 1–33. DOI: 10.1145/3573205.

17. Akinsanya, M., Ekechi, C., & Okeke, C. The evolution of cyber resilience frameworks in network security: a conceptual analysis. *Computer Science & IT Research Journal*, 2024, vol. 5, no. 4, pp. 926–949. DOI: 10.51594/csitrj.v5i4.1081.

18. *Emerging skills and professions for Kazakhstan in the post COVID-19 era*. Available at: https://www.undp.org/kazakhstan/publications/emerging-skills-and-professions-kazakhstan-post-covid-19-era (accessed 13.09.2025).

19. He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*, 2020, vol. 21, no. 2, pp. 203–213. DOI: 10.1108/jic-05-2019-0112.

20. Elmarady, A., & Rahouma, K. Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment. *IEEE Access*, 2021, vol. 9, pp. 143997-144016. DOI: 10.1109/ACCESS.2021.3121230.

21. Marshall, D., Shannon, D., & Love, S. How teachers experienced the COVID-19 transition to remote instruction. *Phi Delta Kappan*, 2020, vol. 102, no. 3, pp. 46–50. DOI: 10.1177/0031721720970702.

22. Lampropoulos, G., Keramopoulos, E., Diamantaras, K., & Evangelidis, G. Integrating Augmented Reality, Gamification, and Serious Games in Computer Science Education. *Education Sciences*, 2023, vol. 13, no. 6, art. no. 618. DOI: 10.3390/educsci13060618.

23. Dos Santos, L., Oliveira, W., Corrêa De Lima, A., De Castro Junior, A., & Hamari, J. The Effects of

Gamification on Learners' Engagement According to Their Gamification User Types. *Technology, Knowledge and Learning*, 2025. DOI: 10.1007/s10758-025-09866-2.

24. Thai, N., De Wever, B., & Valcke, M. Face-to- face, blended, flipped, or online learning environment? Impact on learning performance and student cognitions. *Journal of Computer Assisted Learning*, 2020, vol. 36, no. 3, pp. 397–411. DOI: 10.1111/jcal.12423.

25. Lampropoulos, G. Educational benefits of digital game-based learning: K-12 teachers' perspectives and attitudes. *Advances in Mobile Learning Educational Research*, 2023, vol. 3, no. 2, pp. 805–817. DOI: 10.25082/amler.2023.02.008.

26. Anayatova, R., Tulekova, G., Koshekov, A., Koshekov, K., & Levchenko, N. Professional and Communicative Competences in Using Linguistic Aspects of the State Language in the Sphere of Civil Aviation of Kazakhstan. *PSYCHOLINGUISTICS*, 2024, vol. 36, no. 2, pp. 63–89. DOI: 10.31470/2309-1797-2024-36-2-63-89.

27. *Strategic Cybersecurity Talent Framework*. https://www3.weforum.org/docs/WEF_Strategic_ Cybersecurity_Talent_Framework_2024.pdf (accessed 13.09.2025).

28. *Annual review 2023*. Available at: https://www.iata.org/contentassets/c81222d96c9a4e0bb4ff6ced0126f0bb/annual-review-2023.pdf (accessed 13.09.2025).

29. Willard, J. *Economic impact of cybercrime on business predicted to reach $10.5 trillion by 2025: Cybersecurity Ventures.* Available at: https://www.reinsurancene.ws/economic-impact-of-cybercrime-on-business-predicted-to-reach-10-5-trillion-by-2025-cybersecurity-ventures/#:~:text=The%20economic%20impact%20of%20cybercrime,risk%20appears%20to%20be%20diminishing (accessed 13.09.2025).

30. Florido-Benítez, L. The types of hackers and cyberattacks in the aviation industry. *Journal of Transportation Security*, 2024, vol. 17, art. no. 13. DOI: 10.1007/s12198-024-00281-9.

31. Mizrak, F., & Reyhan Akkartal, G. Prioritizing cybersecurity initiatives in aviation: A dematel-QSFS methodology. *Heliyon*, 2024, vol. 10, no. 16, art. no. e35487. DOI: 10.1016/j.heliyon.2024.e35487.

32. *The cybersecurity industry has an urgent talent shortage. Here's how to plug the gap.* Available at: https://www.weforum.org/stories/2024/04/cybersecurity-industry-talent-shortage-new-report/ (accessed 13.09.2025).

33. *Emerging Trends: ENISA Threat Landscape: From January 2019 to April 2020*. Available at: https://www.enisa.europa.eu/publications/emerging-trends (accessed 13.09.2025).

34. Crumpler, W., & Lewis, J. *The Cybersecurity Workforce Gap*. Available at: https://www.csis.org/analysis/cybersecurity-workforce-gap (accessed 13.09.2025).

35. *Global Cybersecurity Workforce Prepares for an AI-Driven World*. Available at: https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study (accessed 13.09.2025).

36. Gregory, T., & Zierahn, U. When the minimum wage really bites hard: The negative spillover effect on high-skilled workers. *Journal of Public Economics*, 2022, vol. 206, art. no. 104582. DOI: 10.1016/j.jpubeco.2021.104582.

37. Kim, J., & Castelli, D. Effects of Gamification on Behavioral Change in Education: A Meta-Analysis. *International Journal of Environmental Research and Public Health*, 2021, vol. 18, no. 7, art. no. 3550. DOI: 10.3390/ijerph18073550.

38. Pozo-Sánchez, S., Lampropoulos, G., & López-Belmonte, J. Comparing Gamification Models in Higher Education Using Face-to-Face and Virtual Escape Rooms. *Journal of New Approaches in Educational Research*, 2022, vol. 11, pp. 307–322. DOI: 10.7821/naer.2022.7.1025.

39. Kalantayevskaya, N., Koshekov, K., Latypov, S., Savostin, A., & Kunelbayev, M. Design of decision-making support system in power grid dispatch control based on the forecasting of energy consumption. *Cogent Engineering*, 2022, vol. 9, no. 1, art. no. 2026554. DOI: 10.1080/23311916.2022.2026554.

40. *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements.* Available at: https://www.iso.org/standard/27001 (accessed 13.09.2025).

41. *Building a Common Language for Skills at Work A Global Taxonomy*. Available at: https://www.weforum.org/publications/building-a-common-language-for-skills-at-work-a-global-taxonomy/ (accessed 13.09.2025).

42. *Global Skills Taxonomy Adoption Toolkit: Defining a Common Skills Language for a Future-Ready Workforce*. Available at: https://reports.weforum.org/docs/WEF_Global_Skills_Taxonomy_Adoption_Toolkit_2025.pdf (accessed 13.09.2025).

43. Akhavan, M., Alivirdi, M., Jamalpour, A., Kheradranjbar, M., Mafi, A., Jamalpour, R. & Ravanshadnia, M. Impact of Industry 5.0 on the Construction Industry (Construction 5.0): Systematic Literature Review and Bibliometric Analysis. *Buildings*, vol. 15, no. 9, art. no. 1491. DOI: 10.3390/buildings15091491.

44. *Putting Skills First Opportunities for Building Efficient and Equitable Labour Markets*. Available at: https://www.weforum.org/publications/putting-skills-first-opportunities-for-building-efficient-and-equitable-labour-markets/ (accessed 13.09.2025).

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

45. Ghobakhloo, M., Mahdiraji, H. A., Iranmanesh, M., & Jafari-Sadeghi, V. From Industry 4.0 Digital Manufacturing to Industry 5.0 Digital Society: a Roadmap Toward Human-Centric, Sustainable, and Resilient Production. *Information Systems Frontiers*, 2024. https://doi.org/10.1007/s10796-024-10476-z.

46. *Qazaqstan Respublikasynyń enbek narygýn damytýdyń 2024 – 2029 jyldarǵa arnalǵan tújyrimdamasyn bekitý turaly* [On the approval of the Concept for the Development of the Labor Market of the Republic of Kazakhstan for 2024–2029]. Available at: https://adilet.zan.kz/kaz/docs/P2300001050 (accessed 13.09.2025). (In Kazakh).

47. *The Future of Jobs Report 2023*. Available at: https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf?ref=charterworks.com (accessed 13.09.2025).

48. Sabillon, R., & Bermejo Higuera, J. R. The Importance of Cybersecurity Awareness Training in the Aviation Industry for Early Detection of Cyberthreats and Vulnerabilities. *Proceedings of the 25th International Conference on Human-Computer Interaction*, Copenhagen, Denmark, Springer, 2023, pp. 461-479. DOI: 10.1007/978-3-031-48057-7_29.

49. Sabillon, R. Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM. *IGI Global*, 2021, pp. 1-260. DOI: 10.4018/978-1-7998-4162-3.

50. Kolotusha, V., Shmelova, T., & Bondarev, D. Multi-criterion Evaluation of the Criteria of the Information Model Conformity of the Air Traffic Controller Simulator to the Real System. *Lecture Notes in Networks and Systems*, 2024, vol. 992, pp. 364-384. DOI: 10.1007/978-3-031-60196-5_27.

51. Alothman, B. Y. Cyber Gamification: Implementing Gamified Adaptive Learning Environments for Effective Cyber Security Teams Education. *Proceedings of the 5th International Conference on Education Development and Studies*, Cambridge, United Kingdom, Associate of Computing Machinery, 2024, pp. 33-40. DOI: 10.1145/3669947.3669953.

52. Sahnouni, M., & Benghebrid, R. Competency Assessment Based on Fuzzy Logic and Artificial Intelligence Mechanism: A Study of Competency Assessment Document for the Algerian SEROR Company. *Business Ethics and Leadership*, 2023, vol. 7, no. 4, pp. 159–170. DOI: 10.61093/bel.7(4).159-170.2023.

53. Slavyanov, K., & Dimov, R. Application of fuzzy logic in cybersecurity decision making and analysis after a cyber incident detection. *Proceedings of the 15th International Scientific and Practical Conference*, Rezekne, Latvia, 2024, pp. 259–263. DOI: 10.17770/etr2024vol2.8022.

54. Vargas, H., Heradio, R., Farias, G., Lei, Z., & de la Torre., L. A Pragmatic Framework for Assessing Learning Outcomes in Competency-Based Courses. *IEEE Transactions on Education*, 2024, vol. 67, no. 2, pp. 224-244. DOI: 10.1109/TE.2023.3347273.

Received 15.09.2025, Received in revised form 25.12.2025
Accepted date 15.01.2026, Published date 22.01.2026

ГІБРИДНА МОДЕЛЬ ОЦІНКИ КОМПЕТЕНТНОСТЕЙ ПЕРСОНАЛУ СЛУЖБИ З КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВ ЦИВІЛЬНОЇ АВІАЦІЇ З ВИКОРИСТАННЯМ ЕЛЕМЕНТІВ ГЕЙМІФІКАЦІЇ ТА НЕЧІТКОЇ ЛОГІКИ

К. Т. Кошеков, А. К. Сахов, Н. М. Левченко, А. К. Кошеков

Предметом вивчення у статті є підвищення рівня кібербезпеки цивільної авіації за рахунок упровадження гібридної моделі оцінки компетенцій співробітників служби кібербезпеки шляхом використання засобів гейміфікації та нечіткої логіки. **Метою** є розробка гібридної моделі оцінки компетентностей персоналу служби кібер- та інформаційної безпеки підприємств цивільної авіації, заснованої на елементах гейміфікації та нечіткої логіки. **Завдання:** проаналізувати проблему старіння знань і компетенцій фахівців; розробити гібридну модель оцінки компетенцій; обґрунтувати можливість застосування моделі шляхом експериментальної апробації на авіапідприємстві; запропонувати таксономію для формування мінімального набору навичок і компетенцій для оцінки та сертифікації персоналу. Використовуваними **методами** є: нечітка логіка з лінгвістичними змінними та функціями належності; гейміфікація з інтерактивними сценаріями, що імітують кіберінциденти; моделювання із застосуванням правил і процедур дефазифікації; експериментальна перевірка на авіапідприємстві. Отримані такі **результати**: експеримент на авіапідприємствах Республіки Казахстан доводить доцільність застосування даного підходу. Гейміфіковані сценарії, що імітують реальні кіберінциденти, дозволяють в інтерактивній формі й без ризику для реальних систем оцінювати поточний рівень компетентностей персоналу. Штучний інтелект, своєю чергою, забезпечує глибокий аналіз даних, виявляючи індивіду-

альні та системні прогалини у знаннях, а також пропонуючи персоналізовані траєкторії навчання. Дана технологія тестування дозволяє не лише точно вимірювати рівень навичок і компетентностей персоналу, а й своєчасно вживати заходів щодо підвищення кваліфікації. За підсумками дослідження обґрунтовано необхідність розробки таксономії формування портфоліо навичок і компетентностей персоналу служби кібербезпеки авіапідприємств. Така таксономія стане основою для створення стандартизованих норм і критеріїв оцінювання навичок і компетентностей персоналу, на базі яких можна буде проводити об'єктивну оцінку та сертифікацію фахівців із кібербезпеки. До того ж її застосування дозволить своєчасно встановити необхідність підвищення кваліфікації персоналу, що критично важливо в умовах інтенсивно змінюваного кіберландшафту. **Висновки.** Наукова новизна отриманих результатів полягає в такому: 1) розроблено гібридну модель оцінки компетенцій фахівців із кібербезпеки авіаційних підприємств, інтегровану нечіткою логікою та елементами гейміфікації, що забезпечує реалістичну оцінку навичок в умовах динамічного кіберпростору; 2) обґрунтовано методику формування таксономії навичок і компетенцій, яка стане основою для формування стандартизованих норм і критеріїв оцінки (сертифікації); 3) експериментальна апробація моделі на авіапідприємстві підтвердила ефективність у виявленні прогалин у знаннях і дозволила сформувати якісні траєкторії навчання фахівців.

Ключові слова: кіберстійкість; кіберпрофілактика; кіберімунітет; кіберпростір; кіберландшафт; гейміфікація; штучний інтелект; таксономія формування портфоліо компетентностей.

Кошеков Кайрат Темірбаєвич – д-р техн. наук, проф., проф. каф. авіаційної техніки і технологій Академії цивільної авіації, Алмати, Республіка Казахстан.

Сахов Алмат Қайратұлы – маг., асп. каф. авіаційної техніки і технологій Академії цивільної авіації, Алмати, Республіка Казахстан.

Левченко Наталія Михайлівна – д-р держ. упр., проф. Інституту соціології Технічного університету, Берлін, Німеччина.

Кошеков Абай Кайратович – PhD, доц. каф. авіаційної техніки і технологій Академії цивільної авіації, Алмати, Республіка Казахстан.

Kayrat Koshekov – Doctor of Technical Sciences, Professor at the Department of Aviation Technique and Technologies, Civil Aviation Academy, Almaty, Republic of Kazakhstan,
e-mail: kkoshekov@mail.ru, ORCID: 0000-0002-9586-2310, Scopus Author ID: 56150300500.

Almat Sakhov – Master, PhD student of the Department of Aviation Technique and Technologies, Civil Aviation Academy, Almaty, Republic of Kazakhstan,
e-mail: almatsak@gmail.com, ORCID: 0009-0004-0038-3272, Scopus Author ID: 59740601100.

Nataliia Levchenko – Doctor of State Administration, Professor at the Institute of Sociology of the Technical University of Berlin, Germany,
e-mail: levchenkon65@gmail.com, ORCID: 0000-0002-3283-6924, Scopus Author ID: 57258686100.

Abay Koshekov – PhD, Associate Professor at the Department of Aviation Technique and Technologies, Civil Aviation Academy, Almaty, Republic of Kazakhstan,
e-mail: a.k.koshekov@gmail.com, ORCID: 0000-0001-7373-1494, Scopus Author ID: 57192438940.