UDC 004.056 **doi: 10.32620/reks.2025.1.16**

Kayrat KOSHEKOV[1], Baurzhan BAKIROV[1,2], Almat SAKHOV[1], Nataliia LEVCHENKO[3], Yuri TANOVITSKIY[1], Abay KOSHEKOV[1], Yakub KURBANOV[1], Rustam TOGAMBAYEV[4]

[1] *Civil Aviation Academy, Republic of Kazakhstan*
[2] *Aviation administration of Kazakhstan, Republic of Kazakhstan*
[3] *Technical University of Berlin, Germany*
[4] *Transport and Telecommunication Institute, Latvia*

CYBER HYGIENE OF THE DIGITAL TWIN OF THE CIVIL AVIATION OCCUPATIONAL SAFETY MANAGEMENT SYSTEM IN THE CONTEXT OF QUANTUM TRANSFORMATION

*The **subject matter** of this article is cyber hygiene of the digital twin of the occupational safety management system of engineering and technical personnel of civil aviation. The **goal** is to develop a methodology for assessing the cyber hygiene of the digital twin of the occupational safety management system of engineering and technical personnel of civil aviation in the context of transformation into the quantum future. The **tasks**: to develop a methodology for assessing the state of the digital twin of the occupational safety management system of engineering and technical personnel of civil aviation using an integral cyber hygiene index; to develop a model of transitions of the functional state of the digital twin, allowing to predict its cybersecurity, cyber vulnerability and recovery capabilities in case of cyber-attacks; to determine cyber hygiene measures for the digital twin in the context of quantum transformation. **Results**: a methodology for assessing the cyber hygiene of the digital twin of the occupational safety management system of engineering and technical personnel of civil aviation in the context of quantum transformation has been developed; it has been proven that the process of transition of the cyber hygiene system from one state to another, in response to the measures taken, is an iterative process, which allows dynamically monitoring the effectiveness of the taken measures on DT cyber hygiene and predicting its further state; algorithm for the sequence of stages of assessing the state of DT cyber hygiene and their relationship within a cyclic process has been developed. **Conclusions**: a method for assessing the state of DT cyber hygiene has been developed, which, due to its iterative nature and the use of Markov chains, allows determining the probability of the transition of the cyber hygiene system from one state to another, as a response to the measures taken. The application of this method in practice will allow dynamic monitoring of the cyber hygiene of the digital twin and the effectiveness of the measures taken, as well as predicting its future state.*

Keywords: *cyber hygiene; cyberspace; cyber security; cyber incidents; cyber-attacks; cyber well-being; cyber activity; cyber vulnerability.*

1. Introduction

1.1. Motivation

Modern civilization has entered the quantum era - the era of quantum methods of information processing, which are based on the logical concepts of quantum mechanics, providing quantum computers with computing power that is several orders of magnitude greater than the capabilities of modern classical computer technology. This opens up new opportunities and reduces information security, creating prerequisites for cyber threats. The rapid development of quantum technologies and the formation of the quantum industry call for proactive consideration of potential challenges, cyber incidents, and the search for quantum-resistant solutions.

The main goal of creating a digital twin of the occupational safety management system for civil aviation engineering and technical personnel in Kazakhstan is to monitor and prevent the risks of injury and harm to airport personnel's health.

1.2. State of the art

The challenges of quantum transformation are particularly relevant for countries seeking to ensure reliable protection of their digital infrastructures in the context of the global growth of cyber threats. In particular, the Republic of Kazakhstan, according to the

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

Centre for Business Information "Capital" last year, ranked 78th in the world rating for the number of cyber incidents [1].

The rapid growth in the number of incidents in Kazakhstan began in 2023 when the National Computer Emergency Response Team of Kazakhstan (KZ-CERT) recorded an increase in the number of cyber incidents and cyber-attacks to 34.5 thousand cases. The main cyber threats in 2023 were computer viruses, network worms, and Trojans; the number of cyber incidents and cyber-attacks amounted to more than 22 thousand (65%), as well as botnets – the number of cases with which was more than 4 thousand and phishing, which manifested itself in 2.2 thousand cases [2].

In the first half of 2024, the situation only worsened. KZ-CERT found that cybercriminals launched 7.5 times more phishing attacks, and incidents involving viruses, worms, and Trojans increased fourfold. The victims of cybercrime included media (19%), government agencies (12%), financial organizations (12%), telecommunications (7%), logistics and transport (including civil aviation) (7%), and construction (3%). Two-thirds of all attacks on Kazakhstan (65%) were associated with malware, and every second (53%) involved social engineering methods. More than 1/3 of attacks (35%) resulted in the leakage of confidential information. The number of infostealers used by cybercriminals in 2023-2024 includes: The following companies stole personal data: ReadLine, Vidar, Raccoon, Raccoon, Formbook, Agent Tesla, XDigo, Azorult, etc. [1].

According to KZ-CERT reports, four vulnerabilities with the identifiers CVE-2024-28000, CVE-2024-28890, CVE-2023-6000, and CVE-2024-33559 exist on the Kazakhstan segment of the Internet. The most dangerous vulnerability was CVE-2024-28000, which received 9.8 points on the CVSS score. This affects the LiteSpeed Cache plugin and allows attackers to escalate their privileges to create administrator accounts remotely. Many such attacks using this vulnerability are already known [3].

Based on the current situation, KZ-CERT experts assessed the security level of the Kazakhstani corporate cyber environment as below average. Every third company (31%) became a victim of a cyberattack during 2023-2024, and in most cases, they were subjected to DDoS attacks (37%) and malware infections (34%) [2].

To effectively solve the existing problem and adequately respond to the challenges of the modern information society, the globalizing world that has entered the quantum era, the Government of the Republic of Kazakhstan has decided to act decisively. To this end, in March 2023, the Concept of Digital Transformation, Development of the Information and Communication Technologies and Cybersecurity Industry for 2023-2029 [4] was approved, according to which the use of technical means of information protection is currently being expanded, as well as organizational measures are being taken to increase liability for violations in the field of personal data protection and cybersecurity, which will make it possible to counter the growing threats in cyberspace at a higher level, as well as to demonstrate to the world community the desire of the Republic of Kazakhstan to enter the sixth technological order, achieve scientific and technological progress, as well as leadership in digital technologies and the use of artificial intelligence [4].

However, national cybersecurity measures alone are not sufficient. Every company must take a responsible approach to finding quantum-resistant solutions and taking appropriate measures. In addition, companies are especially using digital twin technologies.

Of course, each digital twin has a specific cyber immunity, but this is not sufficient with the rapid development of quantum technologies. It is possible to preserve the health of Digital Twin (DT) only with adequately organized cyber hygiene and a clear understanding of the adoption of necessary measures and their effectiveness, which requires constant knowledge of the state of DT cyber hygiene. Moreover, if someone still gives secondary importance to the issues of DT cyber hygiene, authors should remember that quantum computers are not in the distant future; they are already tomorrow. Therefore, the search for quantum-resistant solutions and the creation of a mature digital twin cyber hygiene systemare already underway.

A review of the literature suggests that academics and practitioners have actively discussed cyber hygiene issues in recent years, even though most companies now implement basic cybersecurity procedures. The number of incidents, such as unauthorized attempts to access systems or data, phishing attacks, malware attacks, and denial of service (DoS) attacks, is continuously increasing [5, 6].

In particular, Juan C. Olivares-Rojas, Enrique Reyes-Archundia, et al. [7] noted that cybersecurity is currently a significant issue due to the digital transformation (DX) driven by information technology (IT), operational technology (OT), and consumer technology (CT) of the fourth industrial revolution (4IR). In addition, as Esparza et al. [8] pointed out, the speed and number of cyberattacks are growing exponentially. In addition, Tuğçe Karayel and Adem Akbıyık [9] concluded that new-generation cyberattacks using artificial intelligence tools are characterized by greater sophistication and effectiveness, which significantly increases their destructive potential.

In particular, Kioskli et al. [10] use the example of critical infrastructure to justify how vulnerable and unprotected it is from cyberattacks, as well as how cyberspace currently exhibits a growing number of challenges related to cybersecurity. The authors emphasized that users must adhere to the rules of cyber hygiene. Moreover, as Fikry et al. [11] emphasized, in an era defined by increased connectivity, understanding and actively implementing sustainable cyber hygiene practices are imperative measures to strengthen the security of the digital landscape of companies. The importance of cyber hygiene is also emphasized by Cain et al. [12]. The authors argued that well-developed cybersecurity risk management and strict cyber hygiene behavior provide cyber resilience and a line of defiance for DT, the demand for which has increased significantly in recent years, according to research by Fabian Böhm et al. [13]. The potential benefits of DT are attracting the attention of several industries, from healthcare to aerospace, because the digital representation of physical assets often enables new business opportunities or critical decisions.

The potential of digital twins has been widely studied (in particular, Koshekov et al. [14]). However, the cybersecurity issues are still of secondary importance, which Holmes et al. [15] emphasized. The authors examined the risks associated with cybersecurity systems using digital twin technology and considered the possibilities of avoiding such risks. In particular, Iqbal H. et al. [16] presented an extensive study of cybersecurity modelling using a taxonomy of artificial intelligence (AI) and explainable AI methods that can help security professionals identify potential threats and incidents and eliminate them in a DT environment in a reasonable manner. Researchers emphasize that it is advisable to be guided by taxonomy, standards, rules, etc., to implement digital twin cyber hygiene measures. The absence of such rules and guidelines for creating mature cybersecurity hygiene, as Ncubukezi et al. [17] argued that this leads to its sluggishness and, accordingly, too painful consequences of cyber incidents and cyberattacks for companies. In this situation, Cain et al. [12] suggested following the cyber hygiene methods recommended by cybersecurity experts. However, Gupta et al. [18] emphasized in their article the fact that generally accepted cyber hygiene recommendations vary significantly in meaning depending on the field of activity of companies, the functional purpose of DT, etc., and therefore can create confusion as to which hygiene measures should be prioritized. In addition, according to Fuskele & Jain [19], when implementing cyber hygiene measures, a set of measures and tools should be used to create a type of DT cybersecurity structure.

Thus, it should be noted that despite numerous recommendations from academic circles to solve the problem of the cyber hygiene of digital twins, this problem continues to exist, thereby creating the requirements for cyber threats.

1.3. Objectives and approach

The object of this study is to develop a methodology for assessing the state of cyber hygiene of a digital twin of the occupational safety management system for civil aviation engineering and technical personnel in the context of transformation to a quantum future. Based on the stated goal, the main objectives are defined as follows: development of a methodology for assessing the state of the digital twin of the occupational safety management system for civil aviation engineering and technical personnel using an integral cyber hygiene index; development of a model for transitions in the functional state of the digital twin, allowing to predict its cyber security, cyber vulnerability and recovery capabilities in case of cyber-attacks; determination of a set of measures for the cyber hygiene of the digital twin in the context of quantum transformation.

The remainder of this article is structured as follows. Section 1: discusses the motivation underlying this study; provides an overview of the state of cyber resilience of digital infrastructures in the context of quantum transformation; and offers an analysis of the latest ideas and methodologies for assessing the state of cyber hygiene of digital infrastructures.

Section 2 describes the materials used to conduct the research, as well as a set of research methods and the stages of their application.

Section 3 presents the results of the step-by-step development of a methodology for assessing the state of cyber hygiene of the digital twin of the occupational safety management system for civil aviation engineering and technical personnel in the context of quantum transformation.

Section 4: presents a discussion of existing methods for assessing the state of cyber hygiene of digital infrastructures, highlights their advantages and disadvantages, the possibility and rationality of scaling in practice; substantiates the feasibility of using the author's method for assessing the state of cyber hygiene of the digital twin of the occupational safety management system of engineering and technical personnel of civil aviation; conducts a comparative analysis with previously proposed methods for assessing the cyber hygiene system, which made it possible to highlight the advantageous aspects of the author's method and its potential impact on increasing the safety level of digital twins in the civil aviation industry.

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

Section 5: presents conclusions based on the research results, and focuses on the practical significance of the author's method for assessing the state of cyber hygiene of the digital twin of the occupational safety management system of engineering and technical personnel of civil aviation in the context of quantum transformation, reveals directions for further research on this topic within the framework of the project "Development of a training complex with an engineering support system for the technical operation of military and special aviation transport equipment".

2. Materials and methods of research

The materials for this study were data from the Information Security Agency of the National Institute of Standards and Technology (NISA); the European Union Agency for Cybersecurity (ENISA); the National Computer Emergency Response Team of Kazakhstan (KZ-CERT); Positive Technologies; the Bureau of National Statistics of the Agency for Strategic Planning and Reforms of the Republic of Kazakhstan and other authoritative sources; the regulatory framework at the international (in particular, ICAO regulations, etc.) and national levels (in particular, regulatory acts of the Republic of Kazakhstan in the field of digital technologies and cybersecurity).

In the course of the research, a comprehensive model for assessing DT cyber hygiene was developed, which includes the following elements: assessing the functional state (cybersecurity and cyber resilience) of a digital twin using the integral Cyber Hygiene Index (CHI); using a model of transitions of the functional state of a DT, which allows predicting cyber security, cyber vulnerability, and the ability to restore its functionality in the event of cyber-attacks; a logical combination of CHI and the model of transitions of the functional state of a digital twin, which makes it possible to form a portfolio of its cyber security and cyber resilience levels, and accordingly determine the necessary measures to improve its cyber hygiene.

The first stage of the study involved collecting data, including key system parameters such as the number of vulnerabilities, frequency of updates, effectiveness of monitoring, and recovery time after an incident. Based on these indicators, the integral CHI index was calculated, which allowed for a quantitative assessment of the patient's condition.

The next step was to model transitions between system states using Markov chains, which made it possible to establish the probabilities of the system transition from one state to another in response to the adopted cyber hygiene measures. It is substantiated that it is the current state of the digital twin's cyber hygiene that determines the system of measures for its hygiene: maintaining the current level of security of the digital twin, making minimal or significant adjustments, and taking measures to eliminate the threat or restore the functionality of the DT system. It has been proven that the DT cyber hygiene process is iterative. Therefore, after each step (taking measures), the system parameters are updated, which means that the CHI index is calculated again, which allows dynamic monitoring of the effectiveness of cyber hygiene measures and prediction of its state. An algorithm for the sequence of stages of the proposed methodology for assessing the state of DT cyber hygiene and their interrelations within a cyclic process is proposed.

3. Results and Discussion

The rapid and avalanche-like introduction of quantum technologies and the formation of the quantum industry motivated us to consider possible cyber incidents and the search for quantum-resistant solutions since cyber incidents are not only the result of technical failures but also deliberate attacks aimed at compromising confidential data, disrupting critical infrastructure, or undermining economic stability [20]. In addition, the cybersecurity measures currently being implemented by governments and businesses are becoming increasingly complex due to the growing sophistication of cybercriminals, fragmentation of the regulatory framework, and the transnational nature of cyber incidents and cyberattacks [21]. Therefore, the issue of cyber hygiene is becoming increasingly relevant.

Note that DT is an advanced technology that provides simulation capabilities to predict, optimize and evaluate system states and configurations entirely digitally along with cyber-physical systems. DT allows the real world to be reproduced in a virtual environment by integrating technologies such as cloud computing and artificial intelligence to generate real-time data. Since DT is at the centre of a significant paradigm shift in Industry 4.0, using this technology provides the opportunity to simulate cyberattacks and protect scenarios without access to the physical environment. However, these capabilities carry some risks because the implicit connection between DT's physical and virtual environments of the DT increases the cyberattack surface. Therefore, DT cybersecurity requires urgent action (Antonio João Gonçalves de Azambuja, Tim Giese [22]). In particular, DT cybersecurity of the safety management system of the engineering and technical personnel of the Republic of Kazakhstan civil aviation.

The issue of creating a DT system for managing occupational safety for civil aviation engineering and technical personnel has become urgent since the number

of air transport workers employed in harmful and hazardous working conditions has been constantly increasing from year to year during 2014–2023 [14], and the measures taken do not ensure the expected effect (Table 1).

According to Table 1, the amount of civil aviation personnel in the Republic of Kazakhstan in 2023 was almost one-and-a-half times higher than in 2014. At the same time, the number of workers employed under harmful and hazardous working conditions, particularly under the influence of increased noise and vibration levels, changed at almost the same rate (see Table 1).

Accordingly, the indicators of labor safety of civil aviation personnel in Kazakhstan during 2014-2023 changed as follows (Table 2).

However, this situation is observed in Kazakhstan's civil aviation and many countries' aviation worldwide.

Table 1

Number of air transport workers engaged in harmful and hazardous work conditions from 2014 to 2023, people [14, 24, 25, 26, 27, 28]

Years	Average number of employees							Number of employees who are entitled to at least one type of compensation				Material concise quinces per victim, million tinge
	Total	of which, employed in harmful and hazardous working conditions										
		including workers	of which are employed on the night shift	employed in conditions that do not meet sanitary and hygienic requirements (standards)	of which working under the influence			Total	of them			
					increased noise and vibration levels	increased dustiness and gas contamination of the air in the working area, exceeding the Maximum permissible concentrations	unfavourable temperature conditions		additional holidays	milk and equivalent food products	additional payments for harmful and other unfavourable working conditions	
2014	6733	3570	1633	590	673	8	4	2633	2444	397	276	718,9
2015	6756	3399	2052	712	723	31	74	2756	2593	139	270	592,7
2016	7054	3011	3043	1355	871	38	-	2965	2741	-	-	587,6
2017	7138	3393	3745	1476	989	47	95	3148	2975	-	-	735,2
2018	7385	3081	3373	2451	1379	59	-	3040	3040	-	-	709,6
2019	8011	3657	3945	3835	2871	51	70	3791	3596	110	496	819,6
2020	7480	2909	4646	2144	2080	31	98	3461	3256	93	425	969,9
2021	7748	2634	4285	2169	2136	34	98	3207	3008	84	288	1236,2
2022	8557	3371	4723	3454	1978	33	93	3589	3402	87	231	1676,9
2023	9231	3459	4811	3567	2012	34	97	3487	3445	89	256	3046,8

Table 2

Occupational safety indicators for civil aviation personnel in the Republic of Kazakhstan during 2014-2023 [14, 24, 25, 26, 27, 28]

Years	Number of victims, people		Injury Frequency Rate (TIFR)	Fatal Injury Frequency Rate (FIFR)	Loss of working time, days		Injury severity coefficient (LTISR)	Total injury rate	Lost Time Injury Rate (LTIFR)
	Total (LTI)	including fatalities			Total	including due to accidents			
2014	274	12	40,6951	1,782266	5757	5757	21,0109	1,9368	23,2623
2015	281	21	41,5927	3,108348	5164	5164	18,3772	2,2632	23,7753
2016	287	16	40,6861	2,268217	5618	5618	19,5749	2,0784	23,2571
2017	303	20	42,4489	2,801905	5535	1479	18,2673	2,3242	24,2648
2018	318	22	43,0603	2,979012	5948	5453	17,1478	2,5111	24,614
2019	312	17	38,9465	2,122082	6788	6386	20,4679	1,9028	22,2627
2020	455	17	60,8289	2,272727	4756	4360	9,58241	6,3479	25,5621
2021	472	17	60,9189	2,194115	5853	5731	12,1419	5,0172	18,2635
2022	127	8	14,8417	0,934907	4933	4843	38,1338	0,3891	8,48385
2023	141	4	24,6731	1,873468	5346	5173	14,5618	2,3515	16,3491

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

According to the International Airport review, a survey of aviation workers conducted by the International Civil Aviation Organization (ICAO) experts in 2022, covering 120 countries, showed that working conditions have worsened for more than 1/3 of aviation employees in recent years. Three-quarters of respondents to the survey organised by the International Transport Workers' Federation (ITF) also reported that the safety of working conditions in aviation has a negative trend with the growth of cargo and passenger transportation [14]. Given the situation's complexity and the urgent need to take measures to improve the working conditions of aviation personnel, the ITF officially presented the "New Deal in Aviation" plan to the ICAO Assembly [23].

Civil aviation in Kazakhstan supports both international initiatives (within the framework of cooperation with ICAO, the Digital Silk Road, etc.) and initiatives of the Government of the Republic of Kazakhstan, in particular, the Concept of Safe Labor in the Republic of Kazakhstan for 2024-2030 [23], adopted within the framework of the Economic Course "Fair Development of Kazakhstan" [14]. Therefore, digital twin technologies of the labor safety management system for engineering and technical personnel have been applied in civil aviation. Using digital technologies today, civil aviation controls personnel's safety and labor protection and creates an environment ready for the future, that is, passenger and cargo transportation growth.

However, with the use of DT technologies, cybersecurity issues have arisen. As previously noted, each digital twin has innate immunity to cyber threats. To ensure such immunity, its architecture includes isolated components, the interaction between which is organized so that an intruder cannot successfully attack any of them. The defeat of these components threatens the system's security as a whole, even in the case of local "successes" of the attack.

However, immunity is prone to change, both to fall with the sophistication of cyber incidents and attacks and to grow with the adoption of cyber hygiene measures. Therefore, to make certain quantum-resistant decisions, it is necessary to clearly understand the state of cyber hygiene of the digital twin. Unfortunately, currently, there are no methods for assessing the state of DT cyber hygiene, and the existing studies on this topic are either fragmentary or incomplete. Therefore, we attempted to solve this problem.

Considering the abovementioned, the authors developed a comprehensive model for assessing the cyber hygiene of the DT of the occupational safety management system for civil aviation engineering and technical personnel, which includes the following elements:

- assessing the functional state (cybersecurity and cyber resilience) of the digital twin using the integral cyber hygiene index (Cyber Hygiene Index, CHI);

- Using the digital twin functional state transition model, which allows predicting cyber security, cyber vulnerability, and the ability to restore its functionality in the event of cyber-attacks;

- a logical combination of CHI and the digital twin functional state transition model, which makes it possible to form a portfolio of the digital twin's cyber security and cyber resilience level and determine the necessary measures to improve its cyber hygiene.

The integral index CNI is an index that assesses the functional state of a digital twin. The CNI index values vary from 0 to 1 as follows:

- Values close to 1 indicate a high level of cybersecurity and the cyber resilience of the digital twin;

- Values close to 0 indicate the existence of cybersecurity and cyber resilience issues that require immediate measures to address the cyber hygiene of the digital twin.

To determine the priority factors influencing the functional state of the digital twin, an expert approach was used, including a multi-step assessment process involving experts in cybersecurity, digital twins, and data analytics.

The study involved 7 experts, including representatives of the Aviation Administration of Kazakhstan, Shymkent International Airport, Petropavlovsk Airport and researchers from the Academy of Civil Aviation of Kazakhstan. The factors were assessed in two stages: at the first, the factors influencing the functional state of the digital twin and its cyber hygiene were identified and prioritised; at the second stage, key factors were ranked by importance through questionnaires and group discussions.

To check the consistency of expert judgments, the Kendall concordance coefficient (W) was used to determine the level of correspondence between expert assessments. The obtained value of $W = 0.82$ indicates a high level of consistency of judgments. Additionally, to check the stability of expert assessments, the coefficient of variation was used, which did not exceed 15% for key factors, confirming their consistency. Thus, the methods used confirm the objectivity and reliability of certain factors in the cyber hygiene index (CHI) calculation model, ensuring the proposed approach's validity.

To calculate CHI, researchers initially identified and prioritized the factors influencing the functional state of the digital twin, with the key factors being:

- Number of vulnerabilities (V) - the number of vulnerabilities detected by the digital twin;

- Patch Frequency (Patch Frequency, F_{patch}) - the frequency of updating the digital twin;

- Monitoring Efficiency (Monitoring Efficiency, E_{det}) - the ability of the digital twin to effectively detect threats;

- Recovery Time (Recovery Time, T_{rec}) the time required to restore the functionality of the digital twin after cyberattacks and the impacts associated with non-traditional threats.

Thus, the formula for calculating CHI takes the following form:

$$CHI = \omega_1 \cdot \frac{1}{V} + \omega_2 \cdot F_{patch} + \omega_3 \cdot E_{det} + \omega_4 \cdot \frac{1}{T_{rec}}, \quad (1)$$

where $\omega_1 = 0.2, \omega_2 = 0.3, \omega_3 = 0.3, \omega_4 = 0.2$ are the weighting coefficients that determines the significance of each of the above factors.

To clearly understand CHI's influence on the change in the state of the digital twin, a decision was made to develop a model of its state transitions. The fundamental basis for constructing this model is the concept of Markov chains, which describe the probability of a system transitioning from one state to another.

Guided by the concept of Markov chains, we established that a digital twin in cybersecurity and cyber resilience can exist in one of the following states (Fig. 1).

Namely, in the state:

- Safe (Safe State, S1) - when the digital twin is cyber-resistant;

- Weak threat (Under Weak Threat, S2) - when potential threats are detected, but the risks are minimal;

- Serious threat (Under Strong Threat, S3) - when threats lead to consequences that require time to restore the digital twin or update it;

- Functionality violations (Breach Detected, S4) - when a cyberattack has led to a malicious impact on the functionality of the digital twin;

- Recovery (Recovery, S5) - when the full restoration of the functionality of the digital twin is underway after a cyber-attack.

To determine the transitions between the states of the digital twin, researchers used a transition matrix P, where each element Pij represents the probability of transition from state i to state j:

$$P = \begin{bmatrix} 0.85 & 0.1 & 0.05 & 0 & 0 \\ 0.1 & 0.7 & 0.15 & 0.05 & 0 \\ 0 & 0.2 & 0.5 & 0.3 & 0 \\ 0 & 0 & 0.3 & 0.4 & 0.3 \\ 0 & 0.1 & 0 & 0.4 & 0.5 \end{bmatrix} \quad (2)$$

Consequently, the parameters (boundaries) of the digital twin of the occupational safety management system for civil aviation engineering and technical personnel were established as follows:

CHI>0.8: S1 (safe state);

0.6<CHI≤0.8: S2 (low threat state);

0.4<CHI≤0.6: S3 (high threat state);

0.2<CHI≤0.4: S4 (functionality impairment state);

CHI≤0.2: S5 (functionality restoration state).

To represent the impact of cyber hygiene on the functional state of the digital twin of the occupational safety management system for civil aviation engineering and technical personnel, a block diagram of the algorithm (Fig. 2) was developed, displaying the main stages of this process and their interrelationships.

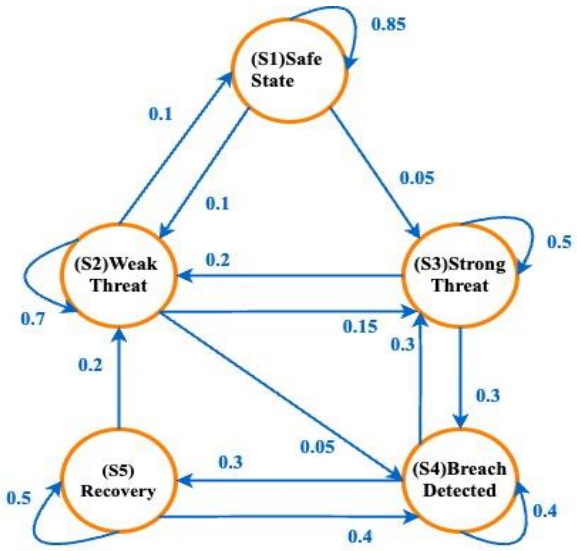


Fig. 1. The structure of the model of transitions between the states of the digital twin of the occupational safety management system for engineering and technical personnel in civil aviation

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

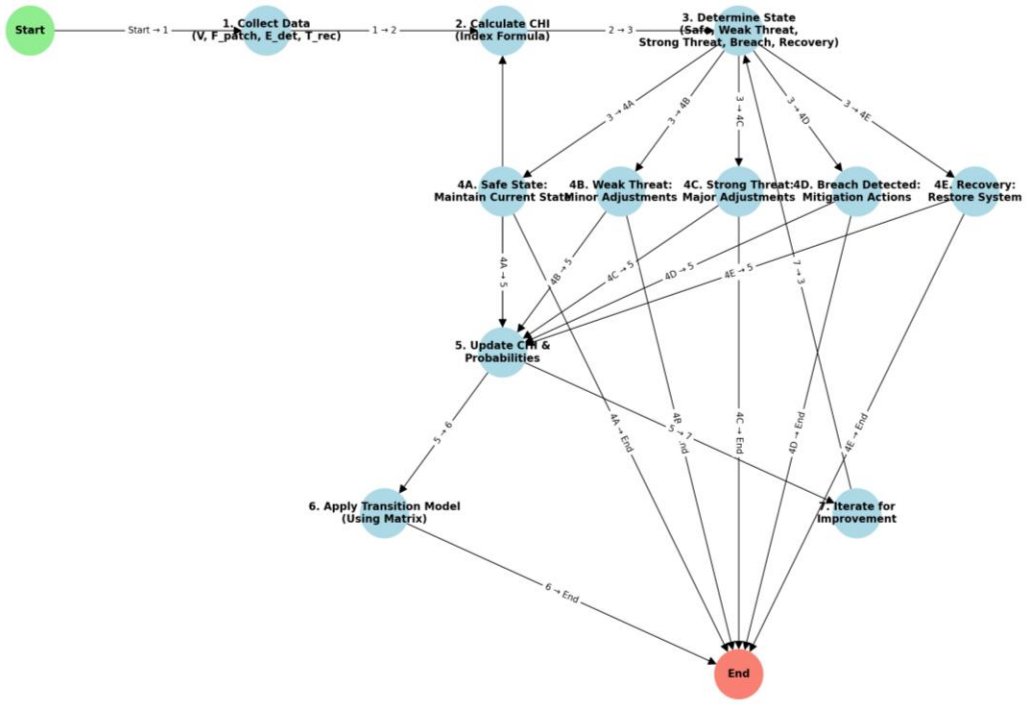


Fig. 2. Algorithm for the cyber hygiene of the digital twin of the occupational safety management system for civil aviation engineering and technical personnel

The initial stage of the proposed algorithm is the collection of data on the cybersecurity and cyber resilience of the digital twin, the number of vulnerabilities, the frequency of updates, the effectiveness of monitoring, its recovery time, etc. The next stage involves calculating the CHI. Based on the CHI value, the current state of cybersecurity and cyber resilience of the digital twin is determined (safe, low threat, high threat, functional impairment or restoration of functionality), which is identified as a fundamental basis for making decisions on its cyber hygiene (i.e. adjustment or restoration). In addition, the implementation of parameter updates and the use of a state transition model are provided, which allows us to diagnose the dynamics of the digital twin state over time.

Figure 2 shows the algorithm in the form of a flow chart with branches, which demonstrates the logical order of actions from the beginning (Start) to the end (End) of the process, including all possible transition scenarios and the cyclic structure for improving the cyber hygiene of the digital twin of the occupational safety management system for civil aviation engineering and technical personnel.

To illustrate the operation of the digital twin functional state transition model, the authors conducted a model experiment to demonstrate the influence of key factors on the CHI and the cybersecurity status of the digital twin.

Stage 1: Initial assessment of the functional state of the digital twin using CHI.

At the initial stage, CHI is used to assess the level of cybersecurity of the digital twin, and the calculation of which the following indicators were collected:

Number of vulnerabilities (V): 8;

Patching frequency (Fpatch): 0.6;

Monitoring efficiency (Edet): 0.7;

Incident recovery time (Trec): 6 hours;

Weighting factors for calculating CHI: $\omega 1=0.2$, $\omega 2=0.3$, $\omega 3=0.3$, $\omega 4=0.2$.

Thus, the CHI was:

$$CHI=0.025+0.18+0.21+0.033=0.4483. \quad (3)$$

The graph (Fig. 3) shows the contribution of each key factor (number of vulnerabilities, patching frequency, monitoring efficiency, and recovery time) to the integrated cyber hygiene index CHI.

Visualization makes it easy to identify which aspects of digital twin cybersecurity require more attention to improve CHI.

Stage 2: Initial state of the system

Given the calculated CHI, researchers can determine the initial functional state of the digital twin.

System state: S3 (substantial threat).

This state is represented as a vector: $\pi 0 = [0,0,1,0,0]$.

Stage 3: Using the state transition model

The state transition model to predict changes in the cybersecurity state of the digital twin. We will use the transition matrix P. A heat map (Fig. 4) is most appropriate for determining the most likely transitions between different systemstates.

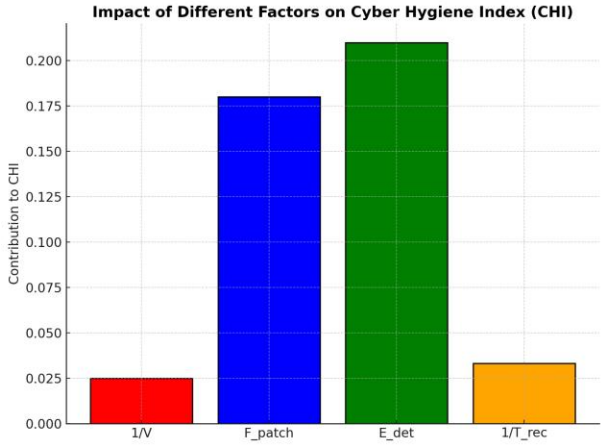


Fig. 3. Impact of key factors on the cyber hygiene index of the digital twin of the occupational safety management system in civil aviation (CHI)

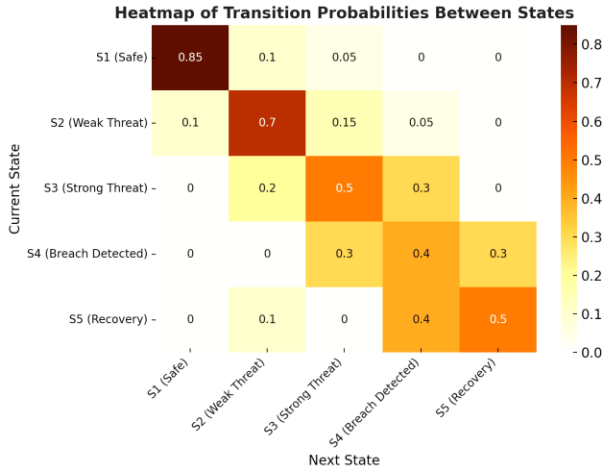


Fig. 4. Heat map of state transitions of the digital twin of the occupational safety management system in civil aviation

The heat map (Fig. 4) provides visual information about which state is accompanied by the greatest threats and thus allows us to determine the necessary measures for the digital twin's cyber hygiene.

Stage 4: The first step in modelling the cybersecurity state of the digital twin.

In the first step, we multiply the initial state vector $\pi 0$ by the transition matrix P as follows:

$$\pi_1 = \pi_0 \cdot P = [0,0,1,0,0] \cdot P = [0, 0.2,0.5,0.3,0]. \quad (4)$$

After the first step, the probabilities of the system being in different states are as follows:

- Probability of being in S2 (low threat): 0.2;
- Probability of being in S3 (high threat): 0.5;
- Probability of being in S4 (functional impairment): 0.3.

Stage 5: Implementing of cyber hygiene measures after the first modelling step

The following measures were taken to improve the state of the digital twin:

- reducing the number of vulnerabilities: after implementing patches, the number of vulnerabilities was reduced from 8 to 4;
- improving the patching frequency: the update frequency was increased from 0.6 to 0.8, indicating regular installation of patches;
- improving monitoring efficiency: monitoring efficiency was increased from 0.7 to 0.85, which helps identify and promptly respond to suspicious activity.

Thus, the updated data was:

Number of vulnerabilities (V): 4;

Patching frequency (Fpatch): 0.8;

Monitoring efficiency (Edet): 0.85;

Incident recovery time (Trec): 6 hours (no change).

Stage 6: Updated CHI Calculation After Digital Twin Cyber Hygiene Measures.

After digital twin cyber hygiene measures, the updated CHI was:

$$CHI = 0.2 \cdot \frac{1}{4} + 0.3 \cdot 0.8 + 0.3 \cdot 0.85 + 0.2 \cdot \frac{1}{6} = 0.05 + 0.24 + 0.255 + 0.0333 = 0.5783 \quad (5)$$

With the updated CHI = 0.5783, the digital twin state is on the verge of transitioning to the S2 (low threat) state, indicating that its cybersecurity level has increased.

Stage 7: The second step of modelling the digital twin cybersecurity state

The updated state vector $\pi 1$ and the transition matrix P are used to determine the state of the digital twin in the second step:

$$\pi_2 = \pi_1 \cdot P = [0,0.2,0.5,0.3,0] \cdot P = = [0.02,0.24,0.37,0.28,0.09] \quad (6)$$

After the calculation, we obtain a new state vector $\pi 2$:

- Probability of being in S1 (safe state): 0.02;
- Probability of being in S2 (weak threat): 0.24;
- Probability of being in S3 (strong threat): 0.37;
- Probability of being in S4 (functional disruptions): 0.28;
- Probability of being in S5 (restoration of functionality): 0.09.

The linear graph (Fig. 5.) reflects the change in the functional state of the digital twin over time. It is evident that at the beginning, the system was in state S3 (Strong Threat), but over time, the states of the digital twin changed depending on the implemented measures.

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

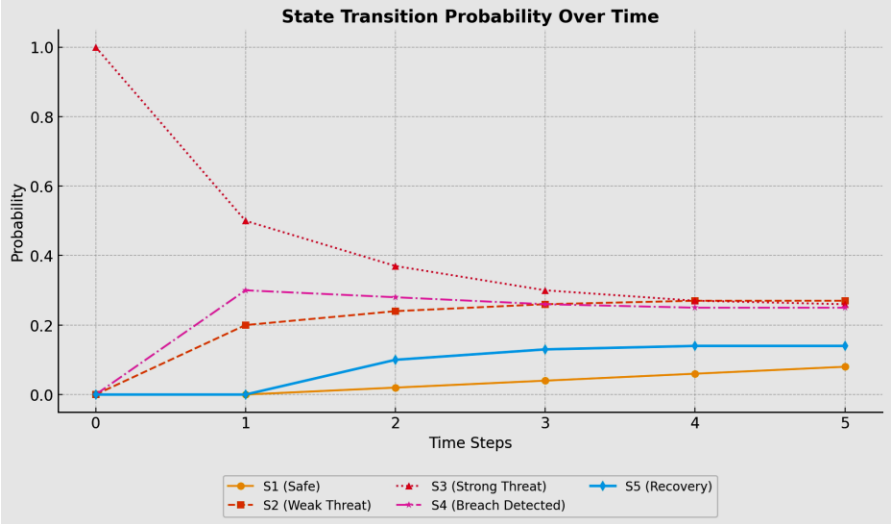


Fig. 5. Changes in the state of the digital twin of the occupational safety management system in civil aviation over time

To demonstrate the effectiveness of the proposed methodology and the dynamics of changes in the system's states, three-dimensional graphs were constructed (Fig. 6a-c). These graphs allow a better understanding of how the system responds to the adoption of cyber hygiene measures, how the probability of a digital twin being in a certain functional state changes, and what changes in state are observed over time. These graphs allow a comprehensive analysis of the probability of a change in the state of a digital twin over time.

In particular, the 3D Bar Plot (Figure 6a) shows the detailed distribution of probabilities at each time step. The 3D Surface Plot (Figure 6b) illustrates the smooth changes between states, and the 3D Line Plot (Figure 6c) focuses on the individual trends of each state. The overall dynamics indicate effective risk mitigation with the adoption of cyber hygiene measures and an increase in the digital twin's cybersecurity level.

Stage 8: Analyzing the impact of the measures taken on the cybersecurity of the digital twin

After implementing cyber hygiene measures, the following dynamics were observed:

The probability of being in S3 (substantial threat) decreased from 0.5 to 0.37. Therefore, improving cyber hygiene has had a positive effect.

The probability of being in S2 (weak threat) increased from 0.2 to 0.24, indicating a tendency to improve the system's state.

The probability of being in S4 (functional impairment) decreased from 0.3 to 0.28, which is also a positive result of reducing the number of vulnerabilities and improving monitoring efficiency.

Thus, protective measures such as reducing the number of vulnerabilities, increasing the frequency of patching and improving the efficiency of monitoring significantly affected the CHI cyber hygiene index, increasing it from 0.4483 to 0.5783.

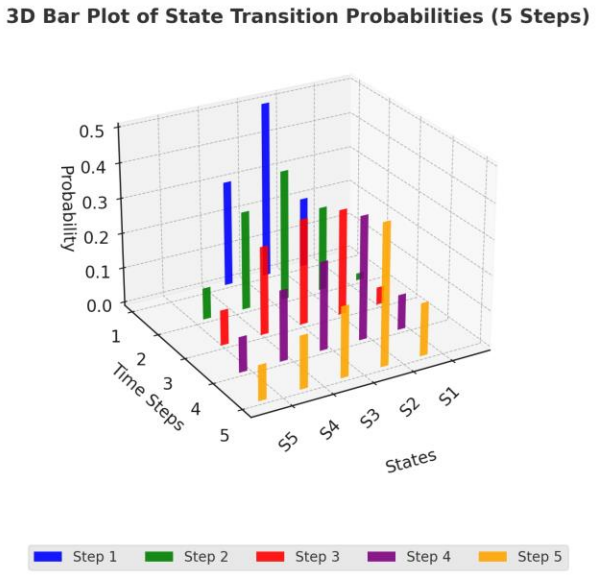
The software implementation of the digital twin cyber hygiene model of the occupational safety management system for civil aviation engineering and technical personnel was implemented in Python (Fig. 7).

The updated state of the system after taking action shows a decrease in the probability of staying in state S3 (high threat) and an increase in the probability of improving to state S2 (low threat).

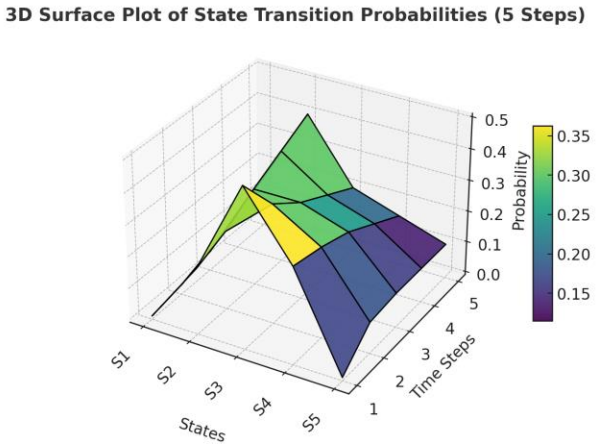
The code consists of the main modules that implement the calculation of CHI, determine the system's state, model transitions between states, and implement protective measures.

The combination of the CHI index and the digital twin state transition model allows us to assess the state of the digital twin cyber hygiene, the effectiveness of the adopted cyber hygiene measures and predict how the digital twin system will respond to the application of specific cyber hygiene measures over time.

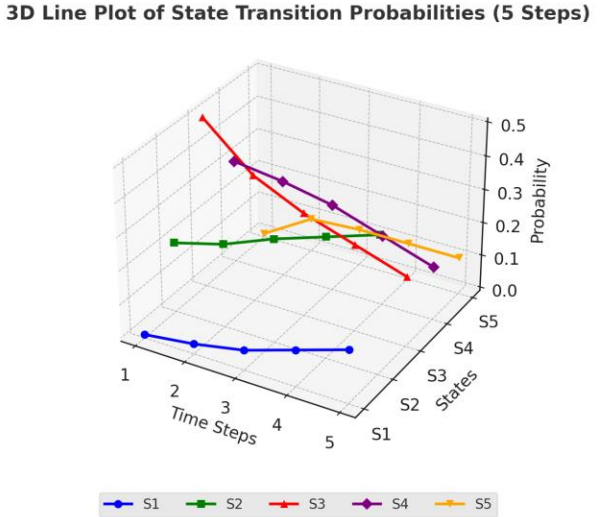
In particular, Gupta & Furnell [18] proposed using the cyber wellness indicator when assessing the state of cyber hygiene. The authors emphasized the need to introduce this indicator into the DT cyber hygiene navigation panel, which offers users a display of the overall cyber wellness status, formed based on aggregation of the subcomponents of the cyber wellness gradient and generalization of status information received from different user devices in the form of a single, agreed value of the cyber wellness indicator; several options for taking measures that can be prioritized to see the most relevant ones; a traffic light system for individual cyber hygiene measures. Green means that the aspect is under control, yellow indicates that more cyber hygiene work needs to be done, and red highlights aspects that require urgent action.



a) 3D bar chart



b) 3D Surface Plot



c) 3D Line Graph

Fig. 6. Three-dimensional graph of the probability of transition of the state of the digital twin of the occupational safety management system for engineering and technical personnel of civil aviation

```python
import numpy as np
def get_transition_matrix():
    return np.array([
        [0.85, 0.1, 0.05, 0, 0],
        [0.1, 0.7, 0.15, 0.05, 0],
        [0, 0.2, 0.5, 0.3, 0],
        [0, 0, 0.3, 0.4, 0.3],
        [0, 0.1, 0, 0.4, 0.5]
    ])
def calculate_chi(V, F_patch, E_det, T_rec, w1=0.2, w2=0.3, w3=0.3, w4=0.2):
    chi = (w1 * (1 / V) + w2 * F_patch + w3 * E_det + w4 * (1 / T_rec))
    return chi
def determine_state(chi):
    if chi > 0.8:
        return "Safe State (S1)"
    elif 0.6 < chi <= 0.8:
        return "Weak Threat (S2)"
    elif 0.4 < chi <= 0.6:
        return "Strong Threat (S3)"
    elif 0.2 < chi <= 0.4:
        return "Breach Detected (S4)"
    else:
        return "Recovery (S5)"
def simulate_transitions(initial_state, P, steps=5):
    state_vector = np.zeros(P.shape[0])
    state_vector[initial_state] = 1
    history = [state_vector]
    for _ in range(steps):
        state_vector = np.dot(state_vector, P)
        history.append(state_vector)
    return np.array(history)
def improve_security(V, F_patch, E_det, T_rec):
    V = max(1, V - 2)
    F_patch = min(1.0, F_patch + 0.1)
    E_det = min(1.0, E_det + 0.1)
    T_rec = max(1, T_rec - 1)
    return V, F_patch, E_det, T_rec
def cyber_hygiene_pipeline(V, F_patch, E_det, T_rec, steps=3):
    print("Starting Cyber Hygiene Analysis...")
    P = get_transition_matrix()
    chi = calculate_chi(V, F_patch, E_det, T_rec)
    state = determine_state(chi)
    print(f"Initial CHI: {chi:.4f}, State: {state}")
    initial_state = ["Safe State (S1)", "Weak Threat (S2)", "Strong Threat (S3)",
                     "Breach Detected (S4)", "Recovery (S5)"].index(state)
    history = simulate_transitions(initial_state, P, steps=steps)
    for step in range(steps):
        print(f"\nStep {step + 1}:")
        print(f"State Probabilities: {history[step]}")
        if state == "Strong Threat (S3)" or state == "Breach Detected (S4)":
            print("Improving Security Measures...")
            V, F_patch, E_det, T_rec = improve_security(V, F_patch, E_det, T_rec)
        chi = calculate_chi(V, F_patch, E_det, T_rec)
        state = determine_state(chi)
        print(f"Updated CHI: {chi:.4f}, Updated State: {state}")
        history = simulate_transitions(initial_state, P, steps=steps)
cyber_hygiene_pipeline(V=8, F_patch=0.6, E_det=0.7, T_rec=6, steps=3)
```

```
Starting Cyber Hygiene Analysis...
Initial CHI: 0.4483, State: Strong Threat (S3)

Step 1:
State Probabilities: [0. 0. 1. 0. 0.]
Improving Security Measures...
Updated CHI: 0.5233, Updated State: Strong Threat (S3)

Step 2:
State Probabilities: [0.  0.2 0.5 0.3 0. ]
Improving Security Measures...
Updated CHI: 0.6100, Updated State: Weak Threat (S2)

Step 3:
State Probabilities: [0.02 0.24 0.37 0.28 0.09]
Updated CHI: 0.6100, Updated State: Weak Threat (S2)
```

Fig. 7. Software implementation of the cyber hygiene model of the digital twin of the occupational safety management system for civil aviation engineering and technical personnel using Python

The proposed methodology for making decisions on implementing cybersecurity measures deserves attention; however, the authors did not disclose the procedure for calculating the cyber well-being indicator, which complicates its practical application.

In addition, the feasibility of its application in specific situations has not been demonstrated. The Software Engineering Institute (SEI) has substantiated the feasibility of using the Cybersecurity Capability Maturity Model (C2M2) by companies, which allows for self-assessment of the cybersecurity program and taking measures to improve it [29, 30].

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

Panda et al. [31], and Deibert [32] recommend using the most optimal security control tool (model) (OST) to assess the state of cyber hygiene. This model combines game theory and combinatorial optimization (0-1 Knapsack), considering the probability of an attack for each user group, the value of assets available to each group, and the effectiveness of each control for a specific group. The model considers indirect costs, such as the time employees may need to learn and prepare for the implemented control. In their opinion, using a game-theoretic framework to support the Knapsack optimization problem allows for the optimal selection of control application levels, minimizing the total expected damage [31].

Skarga-Bandurova et al. [30] propose to use the SPEAR Cyber Hygiene Maturity Model (CHMF) regarding the assessment of the state of cyber hygiene of digital technologies, which allows solving two main tasks in the field of cyber hygiene. First, it ensures an awareness of the state of cyber hygiene. Second, it guides users on the path to taking measures to improve the overall cybersecurity position of the company and achieve maturity in cyber hygiene regarding cybersecurity, privacy, and data protection issues [30, 32, 33, 34].

The approach used by the authors to build SPEAR (CHMF) is a (PDCA) cycle, where P stands for "requirements or plan defined with objectives", D stands for "implementing or performing actions according to plan", C stands for "checking whether the implemented actions work well", and A stands for "action to correct any deviations from the actual achievement of objectives". This approach is consistent with the company's cybersecurity risk management lifecycle described in the NIST Cybersecurity Framework (CSF) [35] and allows companies to improve their cybersecurity capabilities in three different dimensions: organization, infrastructure, and people (Fig. 8) [30, 32, 33, 34].

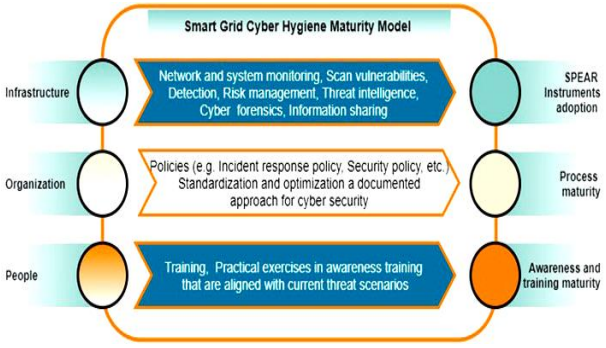


Fig. 8. SPEAR Cyber Hygiene Maturity Model [30]

The digital cyber hygiene assessment result can be used as a cyber health audit to identify countermeasures and re-validate cyber hygiene rules, security standards and specifications [30]. Although this methodology is effective for analyzing "cyber health", it is limited to a static assessment and does not consider the dynamics of system changes in response to implemented security measures.

Another approach proposed by [8] focuses on the human factor in cyber hygiene, particularly developing self-assessment tools to increase user awareness. Although this is an important aspect of cybersecurity, the proposed methodology does not integrate the quantitative analysis of system parameters and dynamic modelling, limiting its effectiveness in complex technical environments.

SPEAR CHMM provides an assessment of the progress of cyber hygiene at five levels (Fig. 9).

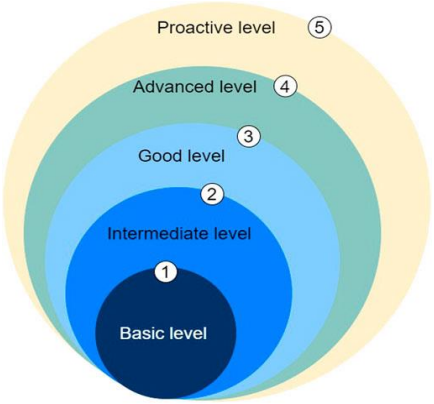


Fig. 9. Five Cyber Levels Hygiene Maturity Model [30]

Compared with the given examples, our developed method for assessing a digital twin's cyber hygiene state is based on quantitatively calculating the cyber hygiene index (CHI) and modelling transitions between system states using Markov chains.

Having collected data, including key system parameters (in particular, the number of vulnerabilities, update frequency, monitoring efficiency, and update time after an incident), an integral CHI index is calculated to quantitatively assess the current state of DT cyber hygiene. The use of which using Markov chains allows modelling transitions between system states and thus determining the probabilities of the system transition from one state to another in response to the adopted cyber hygiene measures. Decisions regarding adopting specific cyber hygiene measures depend on the system's current state and include maintaining the current level of security, making minimal or significant adjustments, taking measures to eliminate threats, or restoring the system's functionality. The experiment proved that this process is iterative, i.e., after each step (measures taken), the system parameters are updated, and the CHI index changes accordingly.

Thus, using the CHI index allows for the dynamic monitoring of the effectiveness of cyber hygiene measures and the prediction of its future status.

The proposed methodology for assessing the state of DT cyber hygiene combines a quantitative approach with dynamic system state modelling, distinguishing it from modern approaches. In addition, compared to the given examples of methods for assessing the state of cyber hygiene, the methodology that was developed has significant advantages due to its iterative nature and the use of Markov chains to model the dynamics of transitions between system states. For example, the methodology [8] focuses on automating risk assessment; however, its approach is limited to static assessments, whereas the proposed methodology allows for predicting the dynamic evolution of a system and adjusting security measures in real-time. This ensures greater flexibility and adaptability (critical in today's cyber environment), continuous monitoring of the system state, and the development of measures to prevent cyber incidents and cyberattacks.

Thus, the proposed methodology for assessing the state of cyber hygiene integrates the best practices of modern approaches and improves them through dynamic assessment, iteration, and forecasting, which allows for a more effective response to DT cyber threats.

Hawdon J. [36], Van Der Zee [37] and other scientists [38, 39, 40, 41, 42] believe that with the development of quantum information processing technologies, it is more expedient to use quantum methods to protect DT, such as quantum key distribution protocols, quantum cryptography, quantum technologies in the field of artificial intelligence, etc. [40, 41], which should be agreed upon to a certain extent. However, the authors are convinced that to counter the cyber threats to DT, it is more expedient to improve the cyber hygiene system through “quantum-resistant” encryption, that is, to protect the system from classical and quantum computers. Alternatively, authors could wait until quantum communication (quantum teleportation) reaches a mature stage and use this quantum technology to protect DT from another quantum technology. However, time is not on our side. The threat already exists [42, 43]. Therefore, researchers consider the best option to be the use of "post-quantum encryption" (PQC), that is, the use of new non-quantum encryption algorithms that even quantum computers cannot solve. In particular, the US National Institute of Standards and Technology (NISA) is already selecting post-quantum encryption algorithms that seek to standardize and apply them worldwide [44, 45].

Thus, based on the results of this study, we conclude that under quantum transformation conditions, for DT cybersecurity and the elimination of vulnerabilities, it is necessary to implement cyber hygiene measures, namely constantly:

- Regular audit of systems and testing of the digital twin for resistance to cyber-attacks. The choice of one or another testing method depends on the purpose, stage of the object's life cycle and the level of maturity of the information security of the digital twin;
- Constant monitoring of the vulnerabilities of the digital twin and their prompt elimination of threats. For this purpose, it is advisable to use SIEM systems (Security Information and Event Management). SIEM system collect and analyse information about security events from various sources in real time. In addition, the use of SIEM in conjunction with NTA or EDR class solutions allows the identification of complex targeted attacks at early stages, thereby ensuring a quick response to existing cyber threats;
- Implementation of intrusion detection systems and behavioral analysis. Participation in bug bounty programs that allow external security researchers to search for new vulnerabilities is recommended. This helps to detect and fix vulnerabilities before attackers use them;
- use of post-quantum encryption algorithms;
- Formation of "soft" standards to attract investment ("the most business-friendly country in the world") in DT cyber hygiene;
- Training employees about DT protection methods.

4. Conclusions

The results of this study make an important contribution to solving the vulnerability of the digital twin of the civil aviation engineering and technical personnel (Digital Twin (DT)) occupational safety management system through the adoption of cyber hygiene measures, the conceptualization and operationalization of which, as well as the empirical assessment of the state of affairs, are essential for the development of a system of measures to reduce the vulnerability of DT under the conditions of quantum transformation.

The study was conducted using a mixed methods approach, which allowed us to develop a methodology for a comprehensive assessment of the state of DT cyber hygiene, which includes the following elements: assessment of the functional state (cybersecurity and cyber resilience) of the digital twin using the integral cyber hygiene index (Cyber Hygiene Index, CHI); use of a digital twin functional state transition model that allows predicting cyber security, cyber vulnerability, and the ability to restore its functionality in the event of cyber-attacks; a logical combination of CHI and a digital twin functional state transition model, which

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

makes it possible to form a portfolio of its cyber security and cyber resilience levels, and accordingly determine the necessary measures to improve its cyber hygiene.

The proposed method for assessing the state of DT cyber hygiene combines a quantitative approach with dynamic modelling of system states, which distinguishes it from modern approaches with significant advantages due to its iterative nature and the use of Markov chains, which allow determining the probabilities of the transition of the cyber hygiene system from one state to another, as a response to the measures taken. During the experiment, it was proven that this process is iterative, i.e. after each step (measures taken), the system parameters are updated, and the CHI index changes accordingly. Thus, using the CHI index allows the dynamic monitoring of the state of DT cyber hygiene, the effectiveness of the measures taken and the prediction of its state in the future.

Further research will be aimed at studying the method of synthesizing digital twins of the occupational safety management system for civil aviation personnel based on digital identification models of production processes.

Contributions of authors: global supervision, conceptualisation, funding acquisition – **Kayrat Koshekov**; methodology development, data acquisition – **Baurzhan Bakirov**; data analysis and visualisation, structuring the model – **Almat Sakhov**; scientific supervision – **Nataliia Levchenko**; structuring the model, programming – **Yuri Tanovitskiy**; CHI algorithm development – **Abay Koshekov**; digital twin system analysis – **Yakub Kurbanov**; programming, data analysis – **Rustam Togambayev**.

Project information: This study is a research project funded by the Ministry of Science and Higher Education of the Republic of Kazakhstan. The goal of the project is to develop, test and implement the technology of designing digital control systems and simulators with an engineering support system for the technical operation of special aviation transport equipment based on 3D modelling and virtual reality to ensure high-quality theoretical and practical training according to the requirements of international standards and recommended practices of ICAO, EASA and IATA.

The control systems and simulators are based on digital twins, and their efficiency and reliability depend on many reasons; however, importantly, on the ability to withstand increasing threats in cyberspace. The research results presented in the article make an important contribution to solving the vulnerability problem of digital twins in civil aviation, the design algorithms of which are studied in the project, thanks to the developed solutions for cyber hygiene, conceptualization, operationalization, and empirical assessment of states.

Conflict of Interest

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

Financing

This research has been funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP19680080). «Development of training complex with a system of engineering support for the technical operation of military and special aviation transport equipment».

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.

References

1. *In the ranking of countries by cybersecurity, Kazakhstan took 78th place*. Available at: https://kapital.kz/tehnology/118681/v-reytinge-stran-po-kiberbezopasnosti-rk-zanyala-78-ye-mesto.html (accessed 12.01.2025). (In Kazakhstan).

2. Domnin, S. *Ne resheto, no sito. Naskolko uyazvim pered kiberatakami kazakhstanskii biznes* [Not a sieve, but a sieve. How vulnerable is Kazakhstani business to cyberattacks]. Available at: https://kz.kursiv.media/2024-06-07/print1037-dmnn-cyber/ (accessed 12.01.2025). (In Kazakhstan).

3. *160 vulnerable WordPress-based websites discovered in the Kazakhstani segment of the Internet*. Available at: https://profit.kz/news/68209/V-Kazahstanskom-segmente-interneta-obnaruzheno-160-uyazvimih-sajtov-na-baze-WordPress (accessed 12.01.2025). (In Kazakhstan).

4. *On approval of the Concept of digital transformation, development of the information and communication technology and cybersecurity industry for 2023-2029*. Resolution of the Government of the Republic of Kazakhstan of March 28, 2023, no. 269. (In Kazakhstan).

5. Ghelani, D., Hua, T. K., & Koduru, S. K. R. Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *American Journal of Computer Science and Technology*, 2022, vol. 10, pp. 1-9. DOI: 10.22541/au.166385206.63311335/v1.

6. Malatji, M. Industrial control systems cybersecurity: Back to basic cyber hygiene practices.

Proceedings of the 2022 International Conference on Electrical, Computer and Energy Technologies, Prague, Czech Republic, IEEE, 2022, pp. 1-7. DOI: 10.1109/ICECET55527.2022.9872810.

7. Olivares-Rojas, J., Reyes-Archundia, E., Gutiérrez-Gnecchi, J. Molina Moreno, I., Mendez Patino, A., & Cerda Jacobo, J. Cyber Hygiene in Smart Metering Systems. *Computación y Sistemas*, 2023, vol. 27, no. 2, pp. 459–475 DOI: 10.13053/CyS-27-2-3894.

8. Esparza, J., Caporusso, N., & Walters, A. Addressing Human Factors in the Design of Cyber Hygiene Self-assessment Tools. *Advances in Intelligent Systems and Computing*, San Diego, CA, USA, Springer, 2020, vol. 1219, pp. 88-94. DOI: 10.1007/978-3-030-52581-1_12.

9. Karayel, T., & Akbıyık, A. Managing Cyber Security Risks and Cyber Hygiene in Organizations: Improving Cyber Resilience. Digital Transformation and Innovation in Emerging Markets. *Digital Transformation and Innovation in Emerging Markets*, 2025, pp. 205-226. DOI: 10.4018/979-8-3373-0086-3.ch010.

10. Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. *Applied Sciences*, 2023, vol. 13, no. 6, art. no. 3410. DOI: 10.3390/app13063410.

11. Fikry, A., Hamzah, M., Hussein, Z., Abdul, A., & Abu Bakar K. Defining the Beauty of Cyber Hygiene: A Retrospective Look. *IEEE Engineering Management Review*, 2024, vol. 52, no. 2, pp. 174-180. DOI: 10.1109/EMR.2024.3361023.

12. Cain, A. A., Edwards, M. E., & Still, J. D. An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 2018, vol. 42, pp. 36–45. DOI: 10.1016/j.jisa.2018.08.002.

13. Böhm, F., Dietz, M., Preindl T., & Pernul, G. Augmented Reality and the Digital Twin: State-of-the-Art and Perspectives for Cybersecurity. *Journal of Cybersecurity and Privacy*, 2021, vol. 1, no. 3, pp. 519-538. DOI: 10.3390/jcp1030026.

14. Koshekov, K., Pirmanov, I., Alibekkyzy, K., Belginova, S., Karymsakova, I., Karmenova, M., & Baidildina, A. Digital twins technology in the educational process of the aviation equipment repair. *Indonesian Journal of Electrical Engineering and Computer Science*, 2023, vol. 32, no. 2, pp. 752-762. DOI: 10.11591/ijeecs.v32.i2.pp752-762.

15. Holmes, D., Papathanasaki, M., Maglaras, L., Ferrag, M., Nepal, S., & Janicke, H. Digital Twins and Cyber Security – solution or challenge? *Proceedings of the 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference*, Preveza, Greece, IEEE, 2021, pp. 1-8, DOI: 10.1109/SEEDA-CECNSM53056.2021.9566277.

16. Sarker, I., Janicke, H., Mohsin, A., Gill, A., & Maglaras, L. Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects. *ICT Express*, 2024, vol. 10, no. 4, pp. 935-958. DOI: 10.1016/j.icte.2024.05.007.

17. Ncubukezi, T., Mwansa, L., & Rocaries, F. A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses. *Proceedings of the 15th International Conference for Internet Technology and Secured Transactions*, London, UK, IEEE, 2020, pp. 1-6. DOI: 10.23919/ICITST51030.2020.9351339.

18. Gupta, S., & Furnell, S. From Cybersecurity Hygiene to Cyber Well-Being. *Lecture Notes in Computer Science*, 2022, vol. 13333, pp. 124-134. DOI: 10.1007/978-3-031-05563-8_9.

19. Fuskele, A.J. Establishing IoT Cyber Hygiene Frameworks with Continuous Monitoring and Risk Assessment in Smart City Infrastructures. *International Journal of Wireless and Ad Hoc Communication*, 2023, vol. 7, no. 2, pp. 41-55. DOI: 10.54216/IJWAC.070203.

20. *Digital Shield: 2023 CYBERSECURITY REVIEW*. Cyber Digest. Available at: https://sts.kz/wp-content/uploads/2024/01/kiberdajdzhest-2023.pdf. (accessed 11.10.2024) (In Kazakhstan).

21. Mokhtar, R., & Rohaizat, A. Cybercrimes and Cyber Security Trends in the New Normal. *The New Normal and Its Impact on Society*, 2024, pp. 41-60. DOI: 10.1007/978-981-97-0527-6_4.

22. Gonçalves de Azambuja, A., Giese, T., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. Digital Twins in Industry 4.0 – Opportunities and challenges related to Cyber Security. *Procedia CIRP*, 2024, vol. 121, pp. 25-30. DOI: 10.1016/j.procir.2023.09.225.

23. *A New Deal for Aviation*. Available at: https://www.itfglobal.org/en/resources/new-deal-aviation. (accessed 11.10.2024)

24. *Number of workers employed in harmful and other unfavorable working conditions in 2023*. Available at: https://stat.gov.kz/en/news/ (accessed 11.10.2024) (In Kazakhstan).

25. *Transport of the Republic of Kazakhstan*. Available at: https://stat.gov.kz/industries/business-statistics/stat-transport/ (accessed 11.10.2024) (In Kazakhstan).

26. *Key labor indicators in the Republic of Kazakhstan*. Available at: https://stat.gov.kz/industries/labor-and-income/stat-wags/ (accessed 11.10.2024) (In Kazakhstan).

27. *On work-related injuries and occupational diseases in the Republic of Kazakhstan*. Available at: https://stat.gov.kz/en/industries/social-statistics/stat-medicine/publications/ (accessed 11.10.2024) (In Kazakhstan).

28. *Social Security Statistics*. Available at: https://stat.gov.kz/industries/social-statistics/stat-medicine/ (accessed 11.10.2024) (In Kazakhstan).

29. *On approval of the Concept of safe labor of the Republic of Kazakhstan for 2024 – 2030*". Resolution of the Government of the Republic of Kazakhstan of December 28, 2023 №1182. (In Kazakhstan).

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

30. Skarga-Bandurova, I., Kotsiuba, I., & Velasco, E. Cyber Hygiene Maturity Assessment Framework for Smart Grid Scenarios. *Frontiers in Computer Science*, 2021, vol. 3, article no. 614337. DOI: 10.3389/fcomp.2021.614337.

31. *Editable CMMC & NIST 800-171 Policies, Standards & Procedures Templates*. Available at: https://complianceforge.com/cmmc-nist-800-171-templates. (accessed 11.10.2024)

32. Deibert J. D. Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs*, 2018, vol. 32, no. 4, pp. 411-424. DOI: 10.1017/S0892679418000618.

33. Panda, S., Panaousis, E., Loukas, G., & Laoudias, C. Optimizing Investments in Cyber Hygiene for Protecting Healthcare Users. *Lecture Notes in Computer Science*, 2020, vol. 12065, pp. 268-291. DOI: 10.1007/978-3-030-41103-9_11.

34. Angelini, M., Bonomi, S., & Palma, A. A Methodology to Support Automatic Cyber Risk Assessment Review. *ArXiv*, 2022. DOI: 10.48550/arXiv.2207.03269.

35. *Cryptographic Module Validation Program*. Available at: https://csrc.nist.gov/projects/cryptographic-module-validation-program. (accessed 11.10.2024)

36. Hawdon, J. Cybercrime: Victimization, perpetration, and techniques. *American Journal of Criminal Justice*, 2021, vol. 46, pp. 837-842. DOI: 10.1007/s12103-021-09652-7.

37. Van Der Zee, S. Shifting the blame? Investigation of user compliance with digital payment regulations. *The human factor in victimization, offending, and policing*, 2021, pp. 61-78. DOI: 10.1007/978-3-030-60527-8_5.

38. Kamar, E., Howell, C. J., Maimon, D., & Berenblum, T. The moderating role of thoughtfully reflective decision-making on the relationship between information security messages and SMiShing victimization: An experiment. *Justice Quarterly*, 2022, vol. 40, no. 6, pp. 837-858. DOI: 10.1080/07418825.2022.2127845.

39. *The Security of Self: A Human-centric Approach to Cybersecurity*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5046484#:~:text=This%20collection%20offers%20a%20new,of%20a%20secure%20cyber%20environment. (accessed 11.10.2024).

40. Al-Hawamleh, A. M. Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures. *International Journal of Advanced Computer Science and Applications*, 2023, vol. 2(14), pp. 801-809. DOI: 10.14569/IJACSA.2023.0140292.

41. Kour, M., & Pierce, J. Cybersecurity Policies Implementation: A Theoretical Model Based on Process Thinking Perspective. *Strengthening Industrial Cybersecurity to Protect Business Intelligence*, 2024, pp. 149-179. DOI: 10.4018/979-8-3693-0839-4.ch007.

42. Kalhoro, S., Rehman, M., Ponnusamy V., & Shaikh F. Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review. *IEEE Access*, 2021, vol. 9, pp. 99339-99363. DOI: 10.1109/ACCESS.2021.3097144.

43. Ainakulov, Z., Pirmanov, I., Koshekov, K., Astapenko, N., Fedorov, I., Zuev, D., & Kurmankulova, G. Risk Assessment of the Operation of Aviation Maintenance Personnel Trained on Virtual Reality Simulators. *Transport and Telecommunication*, 2022, vol. 4(23), pp. 320-333. DOI: 10.2478/ttj-2022-0026.

44. *Quantum technologies in defence & security*. Available at: https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html. (accessed 11.10.2024).

45. Howell, C., Maimon, D., Muniz, C., Kamar, E., & Berenblum, T. Engaging in cyber hygiene: the role of thoughtful decision-making and informational interventions. *Frontiers in Psychology*, 2024, vol. 15, DOI: 10.3389/fpsyg.2024.1372681.

Received 12.01.2025, Accepted 17.02.2025

КІБЕРГІГІЄНА ЦИФРОВОГО ДВІЙНИКА СИСТЕМИ УПРАВЛІННЯ БЕЗПЕКОЮ ПРАЦІ В ЦИВІЛЬНІЙ АВІАЦІЇ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

К. Т. Кошеков, Б. М. Бакіров, А. К. Сахов, Н. М. Левченко, Ю. Н. Тановицький, А. К. Кошеков, Я. М. Курбанов, Р. К. Тогамбаєв

Предметом дослідження є кібергігієна цифрового двійника системи управління охороною праці інженерно-технічного персоналу цивільної авіації. **Ціль** – розробка методології оцінки кібергігієни цифрового двійника системи управління охороною праці ІТП цивільної авіації в контексті трансформації в квантове майбутнє. **Завдання:** розробити методику оцінки стану цифрового двійника системи управління охороною праці ІТП цивільної авіації у вигляді інтегрального індексу кібергігієни; побудувати модель переходів функціонального стану цифрового двійника, що дозволить прогнозувати його кібербезпеку, кіберуразливість та здатність відновлення у разі кібератак; визначити заходи кібергігієни цифрового двійника в умовах глобальної квантової трансформації. **Результати:** розроблено методологію оцінки кібергігієни цифрового двійника системи управління охороною праці ІТП цивільної авіації за умов квантової трансформації; доведено, що процес переходу системи кібергігієни з одного стану в інший, у відповідь на вжиті заходи, є ітераційним процесом, що дозволяє динамічно відстежувати ефективність

вжитих заходів щодо кібергігієни DT та прогнозувати його подальший стан; розроблено блок-схему алгоритму послідовності етапів оцінки стану кібергігієни DT та їх взаємозв'язку в рамках циклічного процесу. **Висновки:** розроблено методику оцінки стану кібергігієни DT, яка завдяки своїй ітеративної природі та використанню ланцюгів Маркова дозволяє визначити ймовірність переходу системи кібергігієни з одного стану в інший, як відповідь на вжиті заходи. Застосування даної методики на практиці дозволить не лише динамічно відслідковувати стан кібергігієні цифрового двійника та ефективність вжитих заходів, а й прогнозувати її зміни в перспективі.

Ключові слова: кібергігієна; кіберпростір; кібербезпека; кіберінциденти; кібератака; кіберблагополуччя; кібердіяльність; кібервразливість.

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

Бакиров Бауржан Маратович – маг., асп. 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.

Тановицкий Юрий Николаевич – канд. техн. наук, наук. співроб. Центру наукових досліджень та компетенцій Академії цивільної авіації, Алмати, Республіка Казахстан.

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

Курбанов Якуб Мухсатұлы – маг., керівник Центру наукових досліджень та компетенцій Академії цивільної авіації, Алмати, Республіка Казахстан.

Тогамбаев Рустам Кумарбекович – маг., асп. Телематика і логістика, Інституту транспорту та зв'язку, Рига, Латвія.

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.

Baurzhan Bakirov – Master, PhD student of the Department of Aviation Technique and Technologies, Civil Aviation Academy, Almaty, Republic of Kazakhstan,
e-mail: b.bakirov@agakaz.kz, ORCID: 0009-0002-9674-5738.

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.

Levchenko Nataliia – 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.

Yuri Tanovitskiy – Candidate of Technical Sciences, Researcher of the Center for Scientific Achievements, Civil Aviation Academy**,** Almaty, Republic of Kazakhstan,
e-mail: y.tanovitskiy@agakaz.kz, ORCID: 0009-0001-5217-1245. Scopus Author ID: 54400321400.

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.

Yakub Kurbanov – Master, Head of the Center for Scientific Achievements, Civil Aviation Academy**,** Almaty, Republic of Kazakhstan,
e-mail: y.kurbanov@agakaz.kz, ORCID: 0000-0002-8883-600X.

Rustam Togambayev – Master, PhD student of the Telematics, Transport and Telecommunication Institute**,** Riga, Latvia,
e-mail: r.togambayev@tsi.lv, ORCID: 0000-0002-0045-5764.