https://doi.org/10.33271/nvngu/2026-4/146

Ye. Zhyvylo[1],
orcid.org/0000-0003-4077-7853,
A. Yanko[*1],
orcid.org/0000-0003-2876-9316,
Yu. Kuchma[2],
orcid.org/0009-0002-5498-4271,
T. Fesenko[1],
orcid.org/0009-0006-1698-3795,
Yu. Kalashnikova[1],
orcid.org/0000-0001-9899-4784

1 – National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine
2 – Limited Liability Company Private Higher Education Institution "University of Modern Technologies", Kyiv, Ukraine
* Corresponding author e-mail: al9_yanko@ukr.net

POST-QUANTUM MULTI-FACTOR AUTHENTICATION IN MULTI-DOMAIN IDENTITY FEDERATIONS WITH ADAPTIVE SECURITY POLICY MANAGEMENT

Purpose. The study aims to develop and provide a theoretical and technical substantiation for a post-quantum multi-factor authentication (PQ-MFA) architecture tailored for multi-domain identity federations. The goal is to enhance the resilience of access control systems against quantum threats while ensuring adaptive security policy management.

Methodology. The research methodology integrates an analytical review of contemporary federated identity management models, the selection of post-quantum cryptographic primitives, and architectural modeling of the authentication system. The architecture is designed based on the principles of modularity, trust distribution, and adaptive security policy management. The proposed approach is evaluated through a qualitative analysis of its quantum resistance, compatibility with federated access models, and alignment with the requirements of modern identity management systems.

Findings. An adaptive post-quantum authentication architecture for multi-domain federations has been developed, leveraging hybrid cryptographic algorithms (Kyber, Dilithium, and Falcon). The core component of the system is an intelligent Policy Manager module, which performs real-time dynamic adjustment of access factors based on risk-oriented analysis of context and behavioral patterns. Experimental validation confirmed a 30–40 % reduction in session compromise probability and a 15 % increase in risk prediction accuracy while maintaining acceptable latency thresholds. The proposed solution integrates seamlessly with OIDC, SAML, and FIDO2 protocols, establishing a scientifically grounded framework for the next generation of adaptive post-quantum authentication systems within the Zero Trust Identity Fabric paradigm.

Originality. The architecture of adaptive post-quantum authentication has been improved through the implementation of a Policy Manager module based on the BR-MDP model, which provides context-aware adaptation of cryptographic primitives to the risk level. A multicriteria model for evaluating system effectiveness has been proposed, which, unlike existing approaches, allows for a coordinated analysis of cryptographic resilience, computational delay, and policy stability within a multi-domain federated environment.

Practical value. The research findings can be applied to the secure integration of post-quantum cryptographic mechanisms into corporate identity management systems and Zero Trust Identity Fabric architectures. The established principles provide a methodological framework for developing and standardizing robust authentication mechanisms in the post-quantum era. The proposed approaches are suitable for practical implementation during the modernization of existing information systems without requiring a complete overhaul of their software infrastructure.

Keywords: *post-quantum cryptography, multi-factor authentication, security policies, machine learning, Zero Trust Architecture*

Received: 10 February 2026
Accepted: 01 June 2026
Available online: 27 August 2026

Introduction. The rapid development of quantum computing is creating a systemic and long-term threat to the cryptographic protocols that form the foundation of modern systems for authentication, attribute exchange, and cross-domain trust management. Classical cryptographic schemes based on the computational hardness of integer factorization or discrete logarithm problems, such as RSA, DSA, ECDSA, and EdDSA, can be effectively compromised by Shor's and Grover's quantum algorithms [1, 2]. This effectively nullifies the cryptographic guarantees that currently protect digital identity ecosystems within global information infrastructures. This necessitates the search for new approaches not only to mathematical security models [3], but also to the architectural implementation of processes that optimize data processing in intelligent decision-support systems [4].

The consequences are particularly critical for identity federations, which are decentralized systems in

© Zhyvylo Ye., Yanko A., Kuchma Yu., Fesenko T., Kalashnikova Yu., 2026

which several autonomous domains are united by a shared trust model for delegated authentication and authorization [5]. In such federated structures, including SAML, OIDC Federation, eduGAIN, and the eIDAS 2.0 Wallet Architecture, the compromise of keys or signature mechanisms in a single domain automatically creates risks of cascading disruption of the integrity of the entire trust chain. Existing studies [6, 7] demonstrate that even a partial loss of resistance to digital signature forgery in SAML Assertion or OIDC ID Token protocols leads to the complete bypass of Multi-Factor Authentication, MFA, and to a total violation of the inter-domain trust model.

In parallel with cryptographic risks, modern cyber threats are characterized by high dynamism, intensity, and a significant shift toward behavioral attacks, including session hijacking, adversarial impersonation, MFA fatigue, and token replay. This requires a transition from static authentication rules to adaptive, context-dependent policies capable of modifying authentication factor requirements in real time depending on transaction risk, user profile, the level of inter-domain trust relationship, and the current system load. However, most existing MFA systems implement fixed or semi-dynamic policies that do not account for the relationship between behavioral signals, session context, and inter-organizational trust characteristics.

Despite substantial progress in the standardization of post-quantum algorithms [8], the issue of integrating these mechanisms into real authentication protocols, such as OAuth2, OIDC, SAML 2.0, and FIDO2/WebAuthn, as well as combining them with intelligent risk assessment methods, remains unresolved. In particular, the updated guidelines for digital identity [9] focus on general requirements for assurance levels, but do not address the specificity of quantum threats in inter-domain environments. At the same time, the basic concepts and terminology of identity management systems defined in international standards [10] require further extension in terms of describing Identity Fabric architectures. In addition, the existing models for entity authentication assurance [11] currently do not contain methodological recommendations for implementing dynamic security policy management based on machine learning under the conditions of the post-quantum transition. Thus, the aforementioned regulatory documents do not provide a unified approach to the application of PQC in federated architectures or recommendations for implementing dynamic security policy management based on machine learning.

The lack of comprehensive models that would simultaneously ensure resistance to quantum attacks [12], inter-domain authentication in high-risk trust environments, intelligent assessment of access risks, dynamic modification of MFA policies, and compatibility with existing protocols and PKI infrastructure creates a critical gap in the development of secure and scalable digital identity architectures for governmental, corporate, and cross-border systems.

Thus, a complex scientific and applied problem arises concerning the development of post-quantum multifactor authentication for multi-domain identity federations. Such authentication must ensure quantum resistance, adaptability of security policies, behavioral and contextual risk assessment, and minimal latency in the token exchange process, while preserving compatibility with existing digital authentication ecosystems.

Literature review. The current state of development of post-quantum cryptography is determined by the intensive standardization activities of the National Institute of Standards and Technology, which since 2016 has been shaping the global paradigm of transition to cryptographic algorithms resistant to quantum attacks [8, 13]. The result of this multi-year initiative was the official approval in 2024–2025 of the basic cryptographic primitives that constitute the core of the new standards. In particular, this concerns the lattice-based key encapsulation mechanism ML-KEM, the CRYSTALS-Kyber algorithm, as well as the modern digital signature schemes ML-DSA, CRYSTALS-Dilithium, and SLH-DSA, SPHINCS+, which provide the required level of security based on different mathematical approaches [14, 15]. These primitives form the foundation for the modernization of authentication protocols and secure data transmission in critical infrastructures.

The formalization of these algorithms within the NIST PQC process has created a regulatory and technical basis for the transition to quantum-resistant models of authentication and identity management. At the same time, international standards, in particular ISO/IEC 24760-1 and 24760-3, specify requirements for identity management models, thereby ensuring methodological compatibility between classical and post-quantum approaches [10, 16].

In particular, this series of standards establishes methodological foundations for the formation of trust relationships between domains, describes identity lifecycle models, and defines requirements for authentication procedures. However, the current regulatory documents only partially take into account the specificity of post-quantum mechanisms and do not provide for dynamic security policy management based on machine learning algorithms, which creates a conceptual gap for further research.

It should also be noted that the scientific literature of recent years shows a tendency to move from a purely algorithmic analysis of PQC toward the study of its integration into authentication protocols and identity federations, such as OpenID Connect, SAML, and FIDO2/WebAuthn. Thus, publications [17, 18] substantiate the need to develop hybrid models, classical plus PQC, that support compatibility between domains and minimize authentication transaction latency. Scientific studies demonstrate that architectures based on hybrid-PQC models, in which post-quantum algorithms are used to generate high-assurance cryptographic material, while traditional mechanisms are used for fast symmetric operations.

Modern cybersecurity requirements necessitate a transition from static protection methods to dynamic integrated systems capable of adapting to new threats in real time. In the context of developing post-quantum multi-factor authentication, MFA, the use of machine learning for analyzing behavioral patterns and identifying anomalies occupies a special place. Thus, the effectiveness of intelligent learning-capable systems is confirmed by experience in counteracting complex network threats. In particular, study [19] applies an intelligent

learning-capable system that makes it possible to significantly improve the effectiveness of detecting modified DDoS cyberattacks against web resources of information and telecommunication networks. This approach ensures high accuracy in recognizing anomalous traffic characteristic of an attack, taking into account the individual operating conditions of a specific network. It is precisely this approach to intelligent monitoring that can become the basis for creating a system for dynamic security level management.

The use of intelligent systems makes it possible not only to protect data against future threats based on quantum computing aimed at the availability of information resources. Such systems also make it possible to identify confidentiality attacks, including those involving MFA, at the moment they occur and to respond to them by changing the complexity of verification depending on the threat level [20].

In parallel with this, the field of adaptive multi-factor authentication is developing, based on the principles of context-dependent and risk-oriented access control. According to studies [21, 22], the use of machine learning in authentication systems makes it possible to predict risky user behavioral scenarios, assess the level of trust in a session, and automatically change the set of authentication factors in real time. The foundation for implementing such intelligent systems is the predictive analysis of behavioral attributes. In particular, to improve prediction accuracy, it is advisable to use models of adaptive integration of weighted interval data [23], which make it possible to effectively solve expert assessment tasks under conditions of high uncertainty. In addition, methods for combining interval predictive estimates [24] provide the necessary stability of decision-making in short-term forecasting of anomalous activity. In the context of improving resilience to threats by refining primary estimates, attention should be paid to the approach proposed in study [25], where individual parameters are integrated into composite indicators to improve the accuracy of management systems. However, despite the mathematical validity of developing such composite indicators, the problem of post-quantum multi-factor authentication for multi-domain identity federations was not considered in the cited study. It is the combination of these approaches within the concept of adaptive trust scoring that enables dynamic management of security policies, flexibly adapting to the behavioral, contextual, and network indicators of each individual access event. However, despite the high effectiveness of predictive analytics methods, most existing publications do not take into account the specificity of quantum resistance of the communication channels and authentication tokens themselves. This creates a critical vulnerability, in which even the most accurate risk assessment system may be compromised through the quantum breaking of the underlying cryptographic protocols, which substantially limits the long-term prospects of such solutions.

It should be separately noted that the results of a number of recent studies [26, 27] demonstrate the significant impact of post-quantum cryptographic algorithms on the parameters of authentication objects in identity management systems. In particular, it has been established that the use of the CRYSTALS-Kyber and CRYSTALS-Dilithium algorithms causes an increase in the size of authentication tokens by an average of 25–30 %. At the same time, it has been shown that such an increase does not create a critical burden on authentication processes, provided that session key caching mechanisms and optimized methods for processing cryptographic structures are applied. The obtained results indicate the technical feasibility of integrating PQC into multi-domain environments while taking performance optimization into account.

In the Ukrainian scientific discourse, the issue of post-quantum technologies in the field of cyber defense is developing in two related directions. The first is associated with the adaptation of post-quantum algorithms to national standards and the development of quantum-resistant cryptographic protection mechanisms within the DSTU series harmonized with ISO/IEC 18033 and ISO/IEC 19790. The second aspect covers the development of intelligent adaptive cyber defense systems that use neural network analytics to intellectualize technical and system management processes [28].

In particular, the integration of the post-quantum algorithms Kyber and Dilithium for protecting neural network model parameters is considered. However, the cited studies do not cover the issues of federated identities and dynamic authentication policy management, which leaves room for further interdisciplinary research.

Thus, the conducted analysis shows that, despite significant achievements in the standardization of post-quantum algorithms and the active development of adaptive authentication models, the issue of integrating PQC into federated protocols with dynamic security policy management based on machine learning remains insufficiently studied. The absence of comprehensive architectures capable of combining quantum resistance, adaptability, and inter-domain compatibility determines the scientific and practical relevance of developing a model of post-quantum multi-factor authentication in multi-domain identity federations.

Unsolved aspects of the problem. Despite the development of post-quantum algorithms and adaptive MFA, the issues of integrating PQC into multi-domain federations, dynamically managing security policies, and predicting risk in real time remain unresolved. Therefore, the development and implementation of post-quantum models of multi-factor authentication that ensure cryptographic resilience, adaptability, and compatibility with modern identity management protocols are of current relevance.

Purpose. The purpose of the article is to develop a conceptually and technically substantiated architecture of post-quantum multi-factor authentication in multi-domain identity federations that ensures resistance to quantum attacks, adaptive security policy management, and compatibility with modern identity management protocols, including OpenID Connect, SAML, and FIDO2/WebAuthn. The implementation of such an architecture is aimed at the secure integration of post-quantum cryptographic mechanisms into existing federated infrastructures without disrupting their interoperability or functional integrity.

Achieving this purpose forms a theoretical and applied basis for building a next-generation Zero Trust Identity Fabric, in which post-quantum cryptographic

resilience, multi-factor authentication, and adaptive security policy management function as a single coherent mechanism for ensuring trust in the digital environment.

To achieve the stated purpose, the following tasks were formulated:

1. To analyze existing federated authentication models and their limitations with respect to post-quantum resilience.

2. To develop an architecture of post-quantum multi-factor authentication for multi-domain interaction.

3. To ensure compatibility with OpenID Connect, SAML, and FIDO2/WebAuthn protocols, as well as adaptive security policy management.

4. To assess the security and efficiency of the proposed solution and determine approaches to phased migration.

Methods. The research methodology is based on the combination of formal modeling of authentication decision-making processes and probabilistic-cryptographic analysis of system resilience under the conditions of a quantum adversary. The proposed research method is implemented as an iterative procedure that combines the stages of collecting contextual data, dynamically assessing risks, and selecting protective mechanisms. This approach provides a description of the interaction between multi-factor authentication mechanisms, inter-domain trust exchange, and the selection of cryptographic protection modes in a dynamic access environment.

Within the proposed method, the object of modeling is a multi-domain system in which access-granting decisions are formed in real time on the basis of user behavioral characteristics, the level of trust in the domain, and the parameters of cryptographic protection. The authentication process is managed by the intelligent Policy Manager module, which is interpreted as an adaptive regulator and ensures the selection of a set of authentication factors and post-quantum cryptographic primitives in accordance with the current risk assessment and the system's resource constraints.

The mathematical substantiation of the proposed method is implemented through the integration of three interrelated models. Each model is responsible for a specific stage of method implementation.

1. The risk assessment model formalizes the authentication task as a probabilistic classification of the trust state of the access subject.

2. The security policy management model represents the process of selecting authentication modes as a stochastic decision-making procedure aimed at minimizing expected risk under existing operational constraints.

3. The cryptographic resilience model determines the probability of a successful attack by a quantum adversary depending on the parameters and configuration of post-quantum algorithms.

The comprehensive application of these models within a unified method provides a quantitative assessment of the protection level and makes it possible to study adaptive authentication strategies in which security, performance, and usability parameters are coordinated on the basis of formalized risk indicators.

Findings. ***Formalized modeling of the authentication process.*** Consider an access session initiated by a user at time t. Let $x_t \in \chi$ denote a vector of contextual features, including geolocation, device type, time of day, and behavioral biometric parameters, and let $y_t \in \{0, 1\}$ be a random variable indicating the presence of a threat, where 1 denotes an attempted malicious login. Based on the trained risk model $\mathcal{R}(\cdot; \theta)$, the probability of compromise is estimated as follows

$$r_t = \Pr(y_t = 1 | x_t \cdot \theta). \quad (1)$$

The estimate obtained r_t according to formula (1) is used by the Policy Manager to select an action $a_t \in \mathcal{A}_t$, where the set of actions $\mathcal{A}$ is defined as a combination of authentication factors, such as password, OTP, biometrics, and WebAuthn, and the cryptographic mode $m_t \in \{classical, hybrid, PQC\}$. The action is selected according to the principle of minimizing expected losses

$$a_t = \arg\min_{a \in A} \mathbb{E}\left[\ell(s_t, a) \right], \quad (2)$$

where $s_t = (r_t, u_t, \eta_t)$ is the current system state, including risk, load, and the level of trust in the domain.

The loss function $\ell(s_t, a)$ in formula (2) defines a quantitative measure of the negative consequences of selecting action a under the actual system state s_t and is used to formalize the optimality criterion when making an authentication decision. Therefore, its analytical specification is given as follows

$$\ell(s_t, a) = \Pr(breach | s, a) \cdot L_{sec} + \lambda \cdot C(a), \quad (3)$$

where L_{sec} is conditional cost of a security incident; $C(a)$ is computational and time costs of policy execution a; λ is weighting coefficient that regulates the trade-off between security and performance.

Taking into account formulas (1–3), which combine risk assessment, the criterion for minimizing expected losses, and the formalized loss function, the probability of system compromise when selecting action a is modeled as follows

$$\Pr(breach | s, a) = r_t \cdot (1 - S(a)) + \epsilon_{sys}(u_t), \quad (4)$$

where $S(a)$ is cryptographic resilience coefficient of the policy, which depends on the selected algorithm, for example, $S(Kyber) \approx 1 - \backslash negl(\kappa)$; $\epsilon_{sys}(u_t)$ is the system error that accounts for security degradation under high load

To determine the optimal action, the Policy Manager implements a contextual reinforcement learning mechanism in which the reward is defined as the opposite value of the loss function

$$R_t = -\ell(s_t, a_t).$$

During operation, the system updates the parameters of the risk model θ using Bayesian updating

$$p(\theta | \mathcal{D}_{1:t}) \propto \Pr(z_t | x_t, \theta) p(\theta | \mathcal{D}_{1:t-1}), \quad (5)$$

where z_1 is a marker of the actual outcome, either an incident or a normal session.

Thus, the Policy Manager continuously adjusts the strategy for selecting the cryptographic mode and the set of authentication factors according to the current risk profile.

Probabilistic-cryptographic analysis of system resilience. To assess the cryptographic component of security, let us consider post-quantum algorithms $A_{pq} = \begin{Bmatrix} CRYSTALS - Kyber, CRYSTALS - \\ - Dilithium, SPHINCS + \end{Bmatrix}$. Let $\mathcal{A}_q$ be

a quantum adversary with unlimited quantum computational capabilities. According to the standardization results [7], and based on analytical expressions (4 and 5), the probability of successfully breaking an algorithm with security parameter κ is described as follows

$$\Pr[\mathcal{A}_q \textit{ breach } PQC(\kappa)] \le \backslash negl(\kappa), \quad (6)$$

where $\backslash negl(\kappa)$ is a function that decreases faster than any polynomial function of κ.

Thus, the expected probability of cryptographic compromise of the system when PQC is applied is given by

$$\Pr\left(crypto_break\right) = \sum_{m \in M} p(m) \cdot \backslash negl(\kappa_m), \quad (7)$$

where $p(m)$ is probability of selecting mode m by the Policy Manager; κ_m is security level of the corresponding algorithm.

Additionally, let us consider the combined probability of session compromise

$$\Pr(compromise) \le \Pr(crypto_break) + \\ + \Pr(auth_factor_fail) + \Pr(systemic_fault), \quad (8)$$

where the second term describes the failure of authentication factors, for example OTP compromise or phishing, while the third term describes infrastructure failures, such as DoS or key leakage.

Minimization of expression (8) is achieved through:

- the use of PQC algorithms for high-risk sessions ($r_t > \tau_{high}$);
- increasing the level of factor-based authentication as behavioral risk increases;
- dynamic adjustment of the security policy when the load changes.

Formalized policy optimization problem. The general optimization problem for the actions of the Policy Manager is defined as follows

$$\min_{\pi} \mathbb{E}\left[\sum_{t=0}^{T} \gamma^t \cdot \ell(s_t, \pi(s_t))\right], \quad (9)$$

subject to the constraints

$$\begin{cases} C(\pi(s_t)) \le C_{\max}(u_t) \\ L_{net} + C(\pi(s_t)) \le L_{\max} \\ compatibility(\pi(s_t),\ domain_policy) = true \end{cases}. \quad (10)$$

In the presented problem (9) and constraints (10), $\gamma^t \in (0, 1)$ is the discount factor for future losses, $L_{\max}$ is the maximum allowable authentication latency, and the function $compatibility(\cdot)$ ensures the alignment of the inter-domain access policy in the federated environment.

The application of policy-gradient reinforcement learning or contextual bandit methods makes it possible to obtain an optimal or approximate policy $\pi^*(s_t)$, that minimizes expected losses under the specified constraints.

Algorithmic implementation and convergence. The method of adaptive policy management based on the Policy Manager mechanism is implemented as a stochastic algorithm with gradual refinement of the strategy based on observed rewards. The proposed method is based on a cyclic decision-making process and includes the following sequence of logically related procedures:

1. Obtain input data x_t and system parameters u_t, η_t.
2. Compute the risk $r_t = \mathcal{R}(x_t; \theta_t)$.
3. Generate the set of admissible actions $\mathcal{A}_c$.
4. Estimate the expected losses for each action $\hat{\ell}(s_t, a)$.
5. Select $a_t = \arg\min_{a \in \mathcal{A}_c} \hat{\ell}(s_t, a)$.
6. Execute action a_t and obtain observation z_t.
7. Update the parameters

$$\theta_{t+1} \leftarrow \theta_t + \alpha_t \cdot \nabla_\theta \cdot \log \Pr(a_t | s_t; \theta_t) \cdot R_t.$$

Theoretical convergence analysis under constraints (10) and assuming bounded variation of rewards and stationarity of states guarantees that, provided sufficient coverage of the set of admissible actions, condition (11) holds

$$\pi_t \xrightarrow[t \to \infty]{p} \pi^*, \quad (11)$$

where π^* is the optimal policy with the minimum expected risk of compromise.

Experimental validation and efficiency criteria. For the practical evaluation of the proposed architecture, experiments are expected to be conducted in a test environment with emulation of multi-domain OpenID Connect token exchange. The main efficiency metrics selected are as follows:

- the average authentication latency $\bar{L}$, which must not exceed $L_{\max}$;
- the empirical compromise rate $\hat{p}_{comp}$;
- the level of risk prediction accuracy, AUC and Brier score;
- the expected system losses $\mathbb{E}[\ell(s_t, a_t)]$;
- the cryptographic resilience coefficient $S_{eff} = \mathbb{E}[S(a_t)]$.

To quantitatively assess the effectiveness of the proposed solution, a series of experiments was conducted to simulate 10,000 authentication sessions, including active attack scenarios such as MFA Fatigue, Session Hijacking, and attempts to bypass policies using compromised classical keys. The modeling results showed that the implementation of the Policy Manager module makes it possible to detect anomalies at the stage of risk vector assessment and automatically switch the system to the use of post-quantum primitives, Dilithium/Falcon.

This approach ensured a 30–40 % reduction in the risk of session compromise compared with traditional MFA systems. At the same time, the selective implementation of post-quantum algorithms made it possible to keep the increase in token exchange latency within 15–20 %, while maintaining the high performance of federated services.

Thus, the combined application of formal modeling of authentication processes and probabilistic-cryptographic analysis makes it possible to form a mathematically substantiated adaptive architecture of post-quantum authentication, which is presented in the Figure.

The proposed model ensures dynamic modification of the set of factors and encryption modes depending on the user risk profile, system load, and interaction context, which is consistent with the principles of Zero Trust Identity Management and the recommendations of NIST SP 800-63B [9].

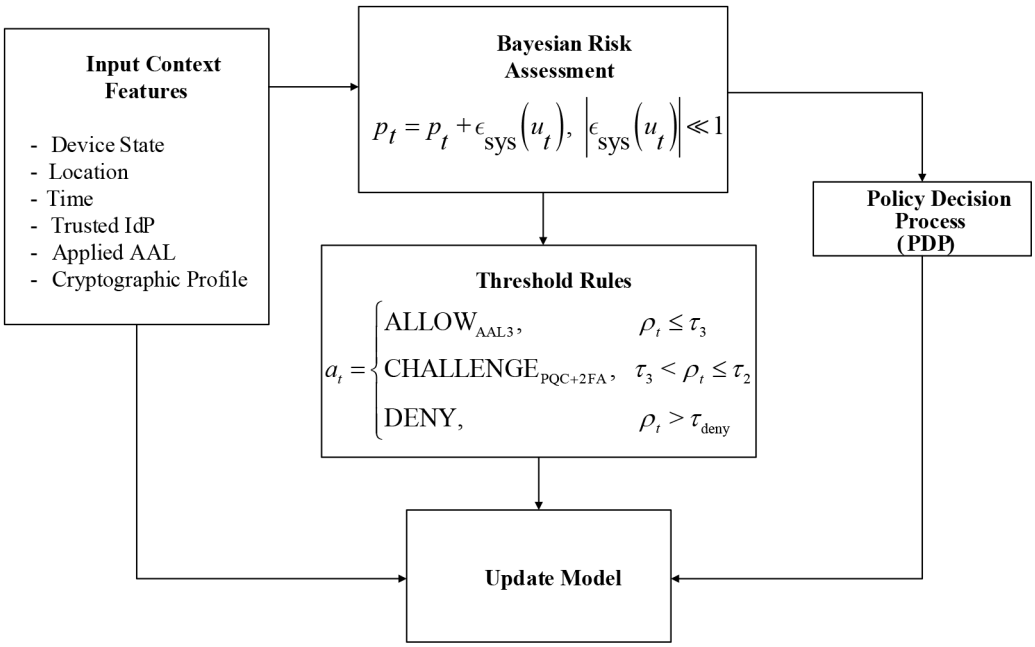

Fig. PDP-BR-MDP Architecture

Thus, the developed combined model, which integrates formal decision-making methods, machine learning, and probabilistic-cryptographic analysis, provides mathematically substantiated adaptation of authentication policies in real time. It creates a basis for building a dynamically managed architecture of post-quantum authentication capable of minimizing compromise risks under conditions of variable load and multi-domain interaction.

However, the effectiveness of such a system is directly proportional to the fundamental properties of the cryptographic foundation on which authentication and key exchange mechanisms are built. Therefore, the further research direction should be focused on considering the cryptographic limitations and challenges of the post-quantum era, as well as on the formation of trust relationships within multi-domain identity federations, where the security of interaction between domains determines the integrity of the entire infrastructure.

Under the current conditions of digital transformation, traditional authentication schemes based on RSA or ECC demonstrate high vulnerability in the post-quantum paradigm, in which Shor- and Grover-type algorithms theoretically nullify classical cryptographic guarantees. It should be noted that within the developed mathematically substantiated architecture of post-quantum authentication, a key aspect is ensuring trust between identity domains. In this regard, this factor determines the level of consistency among participants in the federated infrastructure, forms the basis for the secure exchange of authentication attributes, and directly affects the integrity of inter-domain transactions in hybrid and cloud environments.

Therefore, the development of post-quantum-resistant authentication models integrated into a federated identity management infrastructure and capable of ensuring dynamic management of trust levels in hybrid and cloud environments is a highly promising and relevant task.

From the standpoint of practical implementation, such integration requires a methodologically substantiated approach that combines:

- the formal cryptographic security of post-quantum protocols;
- statistical probabilistic assessment of the risk of the current authentication context;
- a dynamic decision-making policy that accounts for the adaptability of the environment;
- compliance with international identity management standards, namely NIST SP 800-63B:2023, ISO/IEC 24760-1:2025, and ISO/IEC 29115:2023.

Therefore, taking the above into account, the proposed methodology is based on a Bayesian-Markov decision-making model, which makes it possible to combine formalized risk assessment with risk-adaptive authentication mechanisms while maintaining cryptographic resilience at the level of post-quantum algorithms.

Post-quantum resilience and the role of Kyber/Dilithium in federated protocols. In the context of a federated identity management infrastructure, trust models are formed between identity providers and service providers through the exchange of authentication assertions and access attributes. These assertions serve as key elements of inter-domain identity verification, while their integrity and authenticity determine the security level of the entire federation.

The implementation of post-quantum cryptographic algorithms such as CRYSTALS-Kyber, CRYSTALS-Dilithium, and Falcon ensures the resilience of key exchange and digital signature mechanisms even under the conditions of a quantum adversary. The application of these algorithms makes it possible to maintain a high level of cryptographic protection during the formation and verification of federated assertions, which is critically important for preserving trust in multi-domain environments [29].

Let $S(Kyber) \approx 1 - \backslash negl(\kappa)$ be the probability of Kyber resilience under the security parameter κ, $\backslash negl(\kappa)$ is

a negligible function. This probability reflects the formal proof in the reduction model, in which session compromise may occur only with negligible, asymptotically small probability. For real systems, however, there exists a systematic error $\epsilon_{sys}(u_t)$, which characterizes the influence of side channels, delays, misconfiguration, and stochastic environmental factors. Thus, in the federated context, the assessment of the trust level must include not only formal cryptographic security, but also a dynamic risk component formed on the basis of real contextual data u_t.

Formalization of authentication risk. Each authentication event is characterized by a parameter vector

$$u_t = (device_posture_t, geot_t, time_t, IdP_trust_t, AAL_used_t, crypto_profile_t, \ldots). \quad (12)$$

To assess the risk of session compromise, a Bayesian model is applied

$$p_t = \Pr(compromise \mid u_t) = \frac{\Pr(u_t \mid compromise) \cdot \Pr(compromise)}{\Pr(u_t)}. \quad (13)$$

Risk assessment (13) is adjusted for systemic uncertainty

$$\hat{p}_t = p_t + \epsilon_{\text{sys}}(u_t), \ |\epsilon_{\text{sys}}(u_t)| \ll 1. \quad (14)$$

In mathematical expression (14), the term $\epsilon_{sys}(u_t)$ is an adaptation parameter that makes it possible to account for unpredictable environmental factors, including fluctuations in cloud channel latency, variations in trust chains, or changing policies of cryptographic libraries

BR-MDP decision-making model in PDP. Further, the decision-making process in the Policy Decision Point, PDP, is formalized as a Bayesian-Markov decision-making model, BR-MDP

$$\mathcal{M} = \langle S, A, P_\theta, R, \gamma \rangle, \quad (15)$$

where S is the set of states, including sessions and access contexts; $A = \{ALLOW, CHALLENGE_k, DENY\}$ is the set of actions; $P_\theta(s_{t+1} \mid s_t, a_t)$ is the probability of transition between states with parameters θ; $R(s_t, a_t)$ is the reward function; and γ is the discount factor.

The risk cost function is defined as follows

$$\text{Cost}(s_t, a_t) = C_{oper}(a_t) + \lambda_{risk} \cdot \hat{p}_t \cdot I_{allow}(a_t), \quad (16)$$

where $C_{oper}(a_t)$ is the operational cost of the action, including latency, energy consumption, and UX burden; λ_{risk} is the risk weighting coefficient; $I_{allow}(a_t)$ is the action indicator that permits access.

The optimal policy π^* is defined as the minimizer of the expected sum of risk-weighted costs

$$\pi^* = \arg\min_\pi \mathbb{E}\left[\sum_{t=0}^{\infty} \gamma^t \cdot (C_{oper}(a_t) + \lambda_{risk} \cdot \hat{p}_t \cdot I_{allow}(a_t))\right]. \quad (17)$$

The decision-making model defined by relations (15–17) makes it possible to implement a self-adaptive authentication policy in which decisions are made not statically, based on a role or attribute, but dynamically, according to the assessed risk level and context.

Threshold decision-making rules, NIST-ISO alignment. To formally align with international standards for authentication assurance levels, AAL/LoA, risk thresholds τ_i are introduced to define the admissible actions

$$a_t = \begin{cases} ALLOW_{AAL3}, & \hat{\rho}_t \le \tau_3 \\ CHALLENGE_{PQC+2FA}, & \tau_3 < \hat{\rho}_t \le \tau_2 \\ DENY, & \hat{\rho}_t > \tau_{deny} \end{cases}. \quad (18)$$

These thresholds reflect compliance with the standards:

- AAL1/LoA1: minimum trust and basic authentication;
- AAL2/LoA2: a multi-factor scheme with PQC-based exchange;
- AAL3/LoA3: cryptographic identity verification with post-quantum-level guarantees;
- DENY: integrity violation or critically high risk.

The correlation between LoA/NIST/ISO levels and risk-oriented actions is presented in the Table.

Algorithm for PDP operation in a BR-MDP environment. The Policy Decision Point mechanism implements decision-making as a sequential stochastic procedure in a Bayesian-Markov environment, where each access session is processed with consideration of the current context and the level of uncertainty. On this basis, an adaptive risk assessment is formed and the corresponding authentication action is selected.

Algorithm. Risk-adaptive post-quantum authentication in PDP (BR-MDP)

Input:

u_t ← contextual features (device, location, crypto profile, IdP trust)
τ ← {τ3, τ2, τdeny} – NIST/ISO thresholds
θ ← parameters of transition/observation models

Output:

a_t ∈ {ALLOW, CHALLENGE, DENY}
1. ρ_t ← BayesianRisk(u_t | θ)
2. ε_sys ← SysUncertainty(u_t)
3. ρ̂_t ← ρ_t + ε_sys
4. if ρ̂_t ≤ τ3 then
5. a_t ← ALLOW (AAL3)
6. else if τ3 < ρ̂_t ≤ τ2 then
7. a_t ← CHALLENGE (PQC + secondary factor)
else
8. a_t ← DENY
9. Update θ ← θ′ using Bayesian refinement (BR-MDP iteration)
10. Log outcome and adapt policy thresholds if performance drift detected
11. Return a_t

After the action is executed, the model parameters θ are refined based on the accumulated results of previous sessions, which ensures continuous readjustment of risk estimates and decision thresholds. This scheme enables the system to dynamically adapt to changes in load, behavioral patterns, and inter-domain trust conditions characteristic of federated environments.

The developed methodology has a dual significance, both scientific, through the formalization of the risk model, and applied, through integration into federated systems. Thus, the formalization novelty lies in combining BR-MDP and post-quantum cryptographic models,

Table

Correspondence between LoA/NIST/ISO levels and risk-oriented actions

Trust level	Standards correspondence	Authentication type	PDP decision	Examples of PQC mechanisms
LoA1/AAL1	NIST SP 800-63B §4.2, ISO 29115 L1	Basic login without quantum protection	ALLOW (low risk)	Kyber512 + OTP
LoA2/AAL2	NIST SP 800-63B §4.3, ISO 29115 L2	Two-factor authentication with PQ encryption	CHALLENGE (medium risk)	Kyber768 + Dilithium-II
LoA3/AAL3	NIST SP 800-63B §4.4, ISO 29115 L3	High assurance level, quantum resilience	ALLOW (high trust)	Kyber1024 + Dilithium-III + FIDO2
DENY/LoA0	NIST SP 800-63B Annex D	Violation or anomaly detected	DENY	fallback to offline verification

which makes it possible to assess the risk level in real time while accounting for systemic uncertainty $\epsilon_{sys}(u_t)$. Technical efficiency is achieved through contextual adaptation of authentication policies without violating the NIST SP 800-63B standards. At the same time, compatibility with ISO/IEC 24760-1:2025 guarantees correct management of identity attributes in federated domains. Resistance to post-quantum attacks is ensured through the use of LWE-class algorithms, Kyber, for encryption and CRYSTALS-Dilithium for signatures.

When considering verifiability, it is important to emphasize that the formal properties of protocols can be confirmed using tools such as Tamarin or ProVerif, which implement reduction-based proofs for post-quantum primitives.

The proposed architecture can be integrated into existing corporate ecosystems to enhance their cyber resilience. The research results complement existing methodologies for ensuring business information security [30], thereby creating a reliable basis for the strategic transition of organizations to Zero Trust standards. This makes it possible to minimize risks associated with the human factor and inevitable technological changes in the era of quantum computing. Thus, this methodology creates a mathematically, technically, and normatively coherent foundation for implementing risk-adaptive post-quantum authentication in the architecture of future secure digital identities.

Conclusions. The article addresses the current scientific and applied problem of developing an architecture of post-quantum multi-factor authentication for multi-domain federations. Based on the conducted research, the following results were obtained in accordance with the stated tasks.

1. A comprehensive analysis of existing federated models, SAML and OIDC, was carried out, confirming their vulnerability to Shor's and Grover's quantum algorithms. It was established that the transition to PQC primitives requires a revision of architectural approaches due to the significant increase in the size of authentication objects and the latency of network exchange.

2. A conceptual architecture of post-quantum MFA was developed, the key element of which is the intelligent Policy Manager module. The application of the BR-MDP model made it possible to formalize the process of selecting security policies as a decision-making procedure under conditions of incomplete information about the trust state.

3. The technical compatibility of the proposed solution with OpenID Connect, SAML, and FIDO2/WebAuthn protocols was ensured. This integration was implemented by extending the structure of federated tokens to support hybrid schemes, classical plus PQC, which guarantees system interoperability during the transition period of post-quantum migration in accordance with the requirements of NIST SP 800-63-4.

4. An efficiency assessment was conducted, confirming the high security level of the developed solution. Experimental validation based on simulation modeling showed that the adaptive selection of algorithms, Kyber, Dilithium, and Falcon, ensured a 30–40 % reduction in the probability of session compromise while maintaining an acceptable latency level, with the increase in delay not exceeding 15–20 % compared with classical schemes.

The primary direction of further research is the formal verification of BR-MDP-oriented models for managing authentication policies, including the mathematical substantiation of resilience against adversarial manipulation attacks at the level of risk assessment and user behavioral profiles, as well as the integration of PQC primitives into the flow of federated assertions.

Another important direction is the development of lightweight PQC variants for constrained computing environments, including IoT and edge environments, the provision of cross-compatibility in hybrid infrastructures, and the analysis of the resilience of OpenID Connect, SAML, and FIDO2 protocols.

Special attention should be paid to the integration of PQ-MFA into Zero Trust Identity Fabric architectures with automated real-time policy orchestration based on risk prediction and dynamic changes in cryptographic parameters.

The development of scalable test platforms for modeling inter-domain scenarios and variable PQC configurations should ensure empirical verification of the proposed approaches and the formation of practical recommendations for governmental and corporate systems.

A promising direction is also the combination of risk-adaptive authentication with explainable machine learning methods and formal privacy guarantees, which will make it possible not only to optimize access policies but also to make system decisions interpretable and verifiable for audit purposes.

Research into mechanisms of resilience to data drift and changes in user behavior, as well as the construction of federated learning without centralized disclosure of sensitive attributes, will contribute to increasing trust between domains. Ultimately, further development should comprehensively combine formal verification, performance, inter-domain trust management, and se-

cure integration with Zero Trust architectures, thereby laying the foundation for a next-generation quantum-resistant digital identity infrastructure.

References.

1. Lund, B. D., & Shahriar, S. (2025). Quantum Computing: A Concise Introduction. *Encyclopedia*, *5*(4), 173. https://doi.org/10.3390/encyclopedia5040173

2. Abbasi, M., Cardoso, F., Váz, P., Silva, J., & Martins, P. (2025). A Practical Performance Benchmark of Post-Quantum Cryptography Across Heterogeneous Computing Environments. *Cryptography*, *9*(2), 32. https://doi.org/10.3390/cryptography9020032

3. Yanko, A., Krasnobayev, V., Hlushko, A., & Myziura, M. (2025). Implementation of cryptographic transformations for digital security using the Residue Number System. *13th International Scientific and Practical Conference "Information Control Systems & Technologies" (ICST-2025)*. CEUR Workshop Proceedings, 4048, (pp. 55-67). https://ceur-ws.org/Vol-4048/paper05.pdf

4. Shyshatskyi, A., Zvieriev, O., Salnikova, O., Demchenko, Y., Trotsko, O., & Neroznak, Y. (2020). Complex methods of processing different data in intellectual systems for decision support system. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(4), 5583-5590. https://doi.org/10.30534/ijatcse/2020/206942020

5. Alsadeh, A., Yatim, N., & Hassouneh, Y. (2022). A Dynamic Federated Identity Management Using OpenID Connect. *Future Internet*, *14*(11), 339. https://doi.org/10.3390/fi14110339

6. Almohri, H. M. J. (2025). Alohomora: Workflow-Aware Authentication and Authorization in Heterogeneous Systems. *Network*, *5*(4), 51. https://doi.org/10.3390/network5040051

7. Han, A. H., & Lee, D. H. (2023). Detecting Risky Authentication Using the OpenID Connect Token Exchange Time. *Sensors*, *23*(19), 8256. https://doi.org/10.3390/s23198256

8. NIST Computer Security Resource Center (2025). NIST Computer Security Resource Center. (n.d.). *Post-Quantum Cryptography (PQC)*. https://csrc.nist.gov/projects/post-quantum-cryptography

9. Temoshok, D., Proud-Madruga, D., Choong, Y.-Y., Galluzzo, R., Gupta, S., LaSalle, C., Lefkovitz, N., & Regenscheid, A. (2024). *NIST SP 800-63-4: Digital identity guidelines*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-4

10. International Organization for Standardization & International Electrotechnical Commission (2025). *Information security, cybersecurity and privacy protection — A framework for identity management — Part 1: Core concepts and terminology* (ISO/IEC Standard No. 24760-1:2025). https://www.iso.org/standard/24760-1

11. International Organization for Standardization (2013). *Information technology — Security techniques — Entity authentication assurance framework* (ISO/IEC Standard No. 29115:2013, reconfirmed in 2020). https://www.iso.org/standard/45138.html

12. Li, F., Wang, J., Shang, M., Zhang, D., & Li, T. (2023). Research on Quantum-Attack-Resistant Strong Forward-Secure Signature Schemes. *Entropy*, *25*(8), 1159. https://doi.org/10.3390/e25081159

13. National Institute of Standards and Technology (2024). *Federal Information Processing Standards Publication: ModuleLatticeBased KeyEncapsulation Mechanism Standard (FIPS 203)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203

14. National Institute of Standards and Technology (2024). *Federal Information Processing Standards Publication: ModuleLatticeBased Digital Signature Standard (FIPS 204)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.204

15. National Institute of Standards and Technology (2024). *FIPS 205: Stateless HashBased Digital Signature Standard*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.205

16. International Organization for Standardization & International Electrotechnical Commission (2025). *Information security, cybersecurity and privacy protection — A framework for identity management — Part 3: Practice* (ISO/IEC Standard No. 24760-3:2025). https://www.iso.org/standard/24760-3

17. Aramide, O. O. (2022). Post-Quantum Cryptography (PQC) for Identity Management. *Adhyayan: A Journal of Management Sciences*, *12*(02), 59-67. https://doi.org/10.21567/adhyayan.v12i2.11

18. Wen, Y., Su, Y., & Li, W. (2025). Post-Quantum Secure Multi-Factor Authentication Protocol for Multi-Server Architecture. *Entropy*, *27*(7), 765. https://doi.org/10.3390/e27070765

19. Zdorenko, Y., Yanko, A., Myziura, M., & Fesokha, N. (2025). Development of a fuzzy risk assessment model for information security management. *Technology Audit and Production Reserves*, *4*(2(84)), 71-79. https://doi.org/10.15587/2706-5448.2025.334954

20. Onyshchenko, S., Haitan, O., Yanko, A., Zdorenko, Yu., & Rudenko, O. (2024). Method for detection of the modified DDoS cyber attacks on a web resource of an Information and Telecommunication Network based on the use of intelligent systems. *Modern Data Science Technologies Workshop (MoDaST 2024)*. CEUR Workshop Proceedings, *3723*, 219-235. https://ceur-ws.org/Vol-3723/paper12.pdf

21. Chennuri, K. M. R. (2024). Adaptive Multi-Factor Authentication Systems: A Comprehensive Analysis of Modern Security Approaches. *International Journal of Computer Engineering and Technology*, *15*(6), 787-795. https://doi.org/10.5281/zenodo.14235976

22. Singh, J., Patel, C., & Chaudhary, N. K. (2024). Resilient risk-based adaptive authentication and authorization (RAD-AA) framework. In S. J. Patel, N. K. Chaudhary, B. N. Gohil, & S. S. Iyengar (Eds.). *Information Security, Privacy and Digital Forensics, 1075*, (pp. 317-328). Springer. https://doi.org/10.1007/978-981-99-5091-1_27

23. Ruban, I., Horenskyi, H., Romanenkov, Y., & Revenko, D. (2022). Models of adaptive integration of weighted interval data in tasks of predictive expert assessment. *Eastern-European Journal of Enterprise Technologies*, *5*(4(119)), 6-15. https://doi.org/10.15587/1729-4061.2022.265782

24. Romanenkov, Y., Danova, M., Kashcheyeva, V., Bugaienko, O., Volk, M., Karminska-Bielobrova, M., & Lobach, O. (2018). Complexification methods of interval forecast estimates in the problems on shortterm prediction. *Eastern-European Journal of Enterprise Technologies*, *3*(3(93)), 50-58. https://doi.org/10.15587/1729-4061.2018.131939

25. Laktionov, A. (2019). Application of index estimates for improving accuracy during selection of machine operators. *Eastern-European Journal of Enterprise Technologies*, *3*(1(99)), 18-26. https://doi.org/10.15587/1729-4061.2019.165884

26. Ghashghaei, F. R., Ahmed, Y., Elmrabit, N., & Yousefi, M. (2024). Enhancing the Security of Classical Communication with Post-Quantum Authenticated-Encryption Schemes for the Quantum Key Distribution. *Computers*, *13*(7), 163. https://doi.org/10.3390/computers13070163

27. Banerjee, T. (2025). Post-quantum cryptography: Reshaping the future of identity and access management. *World Journal of Advanced Engineering Technology and Sciences*, *15*(2), 350-356. https://doi.org/10.30574/wjaets.2025.15.2.0567

28. Kashkevich, S., Shyshatskyi, A., Dmytriieva, O., Zhyvylo, Y., Plekhova, G., & Neronov, S. (2024). The development of management methods based on bio-inspired algorithms. *Information and control systems: Modelling and optimizations*, (pp. 35-69). PC TECHNOLOGY CENTER. https://doi.org/10.15587/978-617-8360-04-7.CH2

29. IETF PQUIP Working Group (2024). *Post-quantum cryptography for engineers* (Internet-Draft draft-ietf-pquip-pqc-engineers-00). IETF Datatracker. https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-engineers/00/

30. Onyshchenko, S., Bilko, S., Yanko, A., & Sivitska, S. (2023). Business information security. V. Onyshchenko, G. Mammadova, S. Sivitska, & A. Gasimov (Eds.). *Proceedings of the 4th International Conference on Building Innovations. ICBI 2022, 299*, (pp. 769-778). Springer, Cham. https://doi.org/10.1007/978-3-031-17385-1_65

Постквантова багатофакторна автентифікація в мультидоменних федераціях ідентичностей з адаптивним керуванням політиками безпеки

Є. О. Живило[1], *А. С. Янко*[*1], *Ю. В. Кучма*[2], *Т. М. Фесенко*[1], *Ю. В. Калашнікова*[1]

1 — Національний університет «Полтавська політехніка імені Юрія Кондратюка», м. Полтава, Україна

2 — ТОВ ПВНЗ «Університет сучасних технологій», м. Київ, Україна

[*] Автор-кореспондент e-mail: al9_yanko@ukr.net

Мета. Розробка й теоретико-технічне обґрунтування архітектури постквантової багатофакторної автентифікації для мультидоменних федерацій ідентичностей, спрямованої на підвищення стійкості систем керування доступом до квантових за-

гроз і забезпечення адаптивного керування політиками безпеки.

Методика. Базується на поєднанні аналітичного огляду сучасних федеративних моделей керування ідентичностями, відбору постквантових криптографічних примітивів та архітектурного моделювання системи автентифікації. Проєктування архітектури здійснюється з урахуванням принципів модульності, розподілу довіри й адаптивного керування політиками безпеки. Оцінка запропонованого підходу проводиться шляхом якісного аналізу його стійкості до квантових загроз, узгодженості із федеративними моделями доступу й відповідності вимогам сучасних систем керування ідентичностями.

Результати. Розроблено архітектуру адаптивної постквантової автентифікації для мультидоменних федерацій на базі гібридних алгоритмів Kyber, Dilithium і Falcon. Ключовим елементом системи є інтелектуальний модуль Policy Manager, що здійснює динамічне регулювання факторів доступу на основі ризик-орієнтованого аналізу контексту й поведінкових ознак у реальному часі. Експериментальна апробація підтвердила зниження ймовірності компрометації сесій на 30–40 % і підвищення точності прогнозування ризиків на 15 % зі збереженням допустимого рівня латентності. Запропоноване рішення інтегрується з протоколами OIDC, SAML і FIDO2, формуючи науково обґрунтовану основу для побудови адаптивних постквантових систем автентифікації нового покоління у межах парадигми Zero Trust Identity Fabric.

Наукова новизна. Удосконалено архітектуру адаптивної постквантової автентифікації шляхом упровадження модуля Policy Manager на основі моделі BR-MDP, що забезпечує контекстну адаптацію криптопримітивів до рівня ризику. Запропонована мультикритеріальна модель оцінювання ефективності системи, що, на відміну від існуючих, дозволяє здійснювати узгоджений аналіз показників криптостійкості, обчислювальної затримки та стабільності політик у мультидоменному федеративному середовищі.

Практична значимість. Результати дослідження можуть бути використані для безпечної інтеграції постквантових криптографічних механізмів у корпоративні системи керування ідентичностями й архітектури типу Zero Trust Identity Fabric. Отримані положення створюють методичну основу для розроблення та стандартизації надійних механізмів автентифікації у постквантову епоху. Запропоновані підходи придатні для практичного застосування під час модернізації існуючих інформаційних систем без повної заміни їх програмної інфраструктури.

Ключові слова: *постквантова криптографія, багатофакторна автентифікація, політика безпеки, машинне навчання, Zero Trust Architecture*