INNOVATIVE TECHNOLOGICA
METHODICAL RESEARCH JOURNAL
ISSN: 2776-0987 Volume 7, Issue 5, May – 2026

INTEGRATING MODERN CRYPTOGRAPHIC AND ARTIFICIAL INTELLIGENCE-BASED APPROACHES IN INFORMATION SYSTEM SECURITY

G‘ofurova Muxlisa G‘ulom qizi
2nd-Year Student, Information Systems and Technologies
Faculty of Economics and Pedagogy
Tashkent Social Innovation University
muxlisagofurova18@gmail.com
+998-90-358-21-04

Abstract
Modern information systems face a dual threat: conventional cyberattacks and the future threat of quantum computing. This paper analyzes, using the IMRAD method, two key directions in information system protection — modern cryptographic algorithms (AES, TLS, post-quantum NIST standards) and AI-based cybersecurity systems (ML, deep learning, federated learning) — in an integrated framework. Based on research findings, a comprehensive model for integrating these approaches is proposed. In the context of Presidential Decrees PQ-293 (2024), PF-37 (2024), and PQ-358 (2024) of the Republic of Uzbekistan, a four-stage roadmap for strengthening the national information security system is developed.

Keywords: Information security, cryptography, artificial intelligence, TLS protocol, post-quantum cryptography, machine learning, federated learning, NIST standards, hybrid cryptography, cybersecurity integration.

INTRODUCTION

In today's era of rapid digital transformation, protecting information systems is becoming increasingly complex. On one hand, conventional cyberattacks — malware, phishing, DDoS attacks — are intensifying year by year. According to IBM Security's 2024 report, the average global cost of a data breach reached 4.88 million US dollars in 2024 [1]. On the other hand, the advancement of quantum computing poses a serious future threat to cryptographic algorithms currently in use, such as RSA, ECC, and Diffie-Hellman [2].

To address this dual threat, modern information security systems must simultaneously develop in two directions: first, a gradual transition from classical cryptography to post-quantum cryptography; and second, the introduction of

dynamic protection systems based on artificial intelligence. Neither approach alone is sufficient — their synergy provides maximum protection [3].

A number of decrees issued by the President of the Republic of Uzbekistan have elevated both directions to the level of state policy. Presidential Decree PQ-293 (2024) defines objectives for developing the field of cryptology [4], Presidential Decree PF-37 (2024) focuses on strengthening cybersecurity infrastructure, and Presidential Decree PQ-358 (2024) approves the strategy for developing artificial intelligence technologies through 2030 [5]. These documents establish a solid legal foundation for the comprehensive development of the national information security system.

The aim of this paper is to comparatively analyze modern cryptographic methods and AI-based cybersecurity approaches, explore their integration potential, and develop a practical comprehensive protection model for organizations in Uzbekistan.

LITERATURE REVIEW AND METHODOLOGY

Literature Review

In the field of cryptographic protection, the textbook "Cryptographic Methods" authored by Khudoykulov T. et al. (2023) provides a detailed account of the mathematical foundations of cryptography and the practical aspects of AES, RSA, and TLS protocols [6]. Khudoyberdiyev O.T. (TUIT, 2023) analyzed the effectiveness of modern cryptographic algorithms and studied the role of symmetric and asymmetric algorithms in organizational information systems [7]. Karimov N.J. (2022) conducted research dedicated to the security mechanisms of the TLS protocol and its practical applications [8]. G'ofurova M.G'. (2024) performed a comparative analysis of AES, RSA, and TLS algorithms in organizational information systems and evaluated their effectiveness [13].

In the field of post-quantum cryptography, an article published in the "Al-Farghani Descendants" journal by Abdurakhimov B.F., Boyquziyev I.M., and Arabboyev A.A. (2025) analyzed the effectiveness of NIST-standardized algorithms — CRYSTALS-Kyber, Dilithium, FALCON, and SPHINCS+ — in the national context [9]. Shor P.W.'s (1994) algorithm, which proved the possibility of breaking RSA and ECC in polynomial time, demonstrates that the quantum threat is real [2]. G'ofurova M.G'. (2025) developed a practical strategy using NIST standards and hybrid cryptography to protect organizational information systems from quantum threats [14].

ISSN: 2776-0987 Volume 7, Issue 5, May – 2026

On the integration of artificial intelligence and cybersecurity, Achuthan et al. (Frontiers in Big Data, 2024) analyzed AI's role in cryptography, intrusion detection, and privacy preservation. The study emphasizes that the convergence of AI and cryptography will form the foundation of next-generation cybersecurity systems [3]. Bello et al. (IJSRA, 2025) examined the capabilities of supervised and unsupervised learning models in threat detection and automated response, proving that a hybrid approach is the most effective [10].

A study published on Arxiv.org in 2025 examined the issue of "securing cryptography in the age of quantum computing and AI," placing special emphasis on the need to address these two threats not separately but jointly [11].

Research Methodology

The following methods were employed in this study: (1) systematic literature review — based on Uzbek, Russian, and English scientific sources published between 2021 and 2025; (2) comparative evaluation of cryptographic algorithms and AI approaches — using criteria of security, efficiency, and ease of implementation; (3) synthetic analysis of integration models and their adaptation to the national context of Uzbekistan.

Four key criteria were taken into account in the evaluation: (a) security level — resistance to classical and quantum attacks; (b) efficiency — real-time performance and computational cost; (c) adaptability — feasibility of integration with existing infrastructure; (d) national compliance — conformity with the laws and standards of Uzbekistan.

RESULTS

Comparative Analysis of Cryptographic and AI-Based Protection Methods

Modern methods used to protect information systems can be divided into three groups: classical cryptographic algorithms, post-quantum algorithms, and AI-based dynamic protection systems. Each group has its own distinctive advantages along with certain limitations.

INNOVATIVE TECHNOLOGICA
METHODICAL RESEARCH JOURNAL
ISSN: 2776-0987 Volume 7, Issue 5, May – 2026

Table 1. Comparative analysis of information system protection methods [2, 6, 7, 9, 10]

Protection Method	Basis	Advantages	Disadvantages	Application
AES-256 (Symmetric)	Mathematical algorithm	Fast, efficient	Complex key management	Data storage
RSA-2048 (Asymmetric)	Large-number factorization	Public key infrastructure	Vulnerable to quantum computers	Key exchange
TLS 1.3 Protocol	Hybrid cryptography	Network security	Complex configuration	HTTPS, VPN
ML-based IDS	Machine learning	Detects unknown threats	Requires training data	Network monitoring
Post-quantum (Kyber)	Lattice theory	Quantum-resistant	Not yet widely deployed	Future systems
Hybrid (classical+PQC+AI)	Comprehensive approach	Multi-layered protection	Cost and complexity	Critical systems

As shown in the table, no single method can provide complete protection against all threats. While symmetric encryption (AES-256) is ideal for data storage, the challenge of key management remains. RSA asymmetric cryptography is widely used in key exchange, but faces the threat of quantum computers. Although TLS 1.3 ensures network security, an additional AI layer is required against hybrid attacks [7, 8].

Post-quantum algorithms (Kyber, Dilithium) are the primary tools for defending against quantum threats, yet they are not yet widely deployed and practical experience remains limited. For this reason, a hybrid approach — combining classical cryptography, post-quantum algorithms, and AI systems — is currently considered the most optimal solution [3, 9].

Key Models for Integrating AI and Cryptography

In the course of this research, five key models for combining AI and cryptography were identified. Each model addresses different organizational needs.

INNOVATIVE TECHNOLOGICA
METHODICAL RESEARCH JOURNAL
ISSN: 2776-0987 Volume 7, Issue 5, May – 2026

Table 2. Integration models of AI and cryptography [3, 9, 10, 11]

Integration Model	Cryptographic Basis	AI Component	Effectiveness	Application Area
AI-cryptographic key management	AES, RSA	Anomaly detection (ML)	Key security improves by 40%	Finance, government
AI-enhanced TLS	TLS 1.3	Real-time threat detection	Attack response 60% faster	Web applications
PQC + Federated Learning	CRYSTALS-Kyber	Distributed training	Privacy + quantum resistance	Cloud systems
XAI + Digital Signature	Dilithium (FIPS 204)	Explainable AI	Audit and transparency	Legal systems
Hybrid cryptography + DL	RSA + Kyber (parallel)	Deep learning analysis	Backward compatibility + security	Transition period

The AI-cryptographic key management model is particularly significant — research has proven that ML algorithms can detect anomalies in real time during key generation, distribution, and renewal, improving key security by 40% [3]. The AI-enhanced TLS model adds a machine learning layer on top of the traditional TLS 1.3 protocol, reducing attack response time by 60% [10].

The combination of PQC and federated learning is especially promising for cloud-based and distributed systems — it enables secure training of data in a decentralized manner, ensuring both quantum resistance and privacy [9, 11].

DISCUSSION

Synergistic Effect of Integration

It is insufficient to consider cryptographic and AI-based approaches separately — their combined effect (synergistic effect) exceeds the sum of their individual indicators. In particular, an ML-based anomaly detection system can identify malicious behavior even within encrypted traffic — something that was not possible with classical cryptography alone. Conversely, cryptographic protection safeguards the confidential data used to train AI models from unauthorized access [3, 11].

Achuthan et al. (2024) emphasized that this integration gives rise to the concept of "intellectually empowered cryptographic protection": cryptography serves as the foundation of protection, while AI acts as its adaptive "brain." This approach enables the detection of zero-day vulnerability attacks with 70–85% accuracy [3].

INNOVATIVE TECHNOLOGICA
METHODICAL RESEARCH JOURNAL
ISSN: 2776-0987 Volume 7, Issue 5, May – 2026

A Comprehensive Approach Against the Quantum Threat

The "Harvest Now, Decrypt Later" threat remains one of the most pressing challenges in information security. Encrypted data being collected today may be decrypted in the future using quantum computers. This is particularly dangerous for state secrets and long-term confidential corporate data [2].

AI systems are assigned a special role in combating this threat: ML models can detect "abnormal" data collection behavior, while federated learning can ensure that confidential data is stored in a decentralized manner. At the same time, by introducing post-quantum algorithms, it becomes possible to proactively defend against future quantum attacks [9, 11].

Comprehensive Implementation Strategy in the Context of Uzbekistan

Three important documents of Uzbekistan — PQ-293 on cryptology, PF-37 on cybersecurity, and PQ-358 on artificial intelligence — define independent development directions. However, to achieve the most effective outcome, all three directions must be implemented jointly, in an integrated manner.

Table 3. Roadmap for cryptography and AI integration for Uzbekistan organizations [4, 5, 9, 10]

Stage	Timeline	Cryptographic Measure	AI Integration	Legal Basis
1. Inventory and analysis	0–6 months	Audit existing AES/RSA systems	Identify vulnerabilities using ML	PQ-293 (2024) – cryptology
2. AI and TLS strengthening	6–18 months	Deploy TLS 1.3, renew certificates	Install IDS/SIEM systems	PF-37 (2024) – cybersecurity
3. Transition to hybrid cryptography	18–36 months	RSA + Kyber parallel operation	Introduce federated learning	PQ-358 (2024) – AI strategy
4. Full PQC + AI integration	36+ months	NIST FIPS 203–206 standards	Audit and monitoring via XAI	UzDst national standards

Companies operating within the IT Park Uzbekistan system have the opportunity to implement the first two stages of this roadmap more quickly — as these residents

have access to modern infrastructure and international expertise. G‘ofurova M.G‘. (2025) showed in her research that information security plays an important role in the IT export and startup ecosystem development activities of IT Park resident companies [15]. Strengthening security standards under the "Zero Risk" program creates a favorable platform for a comprehensive approach.

As noted in a study by Khudoykulov Z. et al. (IEEE ICESC, 2023), authentication issues in cloud computing systems remain unresolved, requiring additional attention when implementing AI-based cybersecurity systems [12]. An additional challenge for national organizations is the limited availability of cybersecurity datasets in the Uzbek language, which makes training AI models more difficult.

CONCLUSION

This research has led to the following key conclusions:

1. In information system protection, cryptographic methods and AI-based approaches are complementary yet individually insufficient tools. Their integration — intellectual protection built on a cryptographic foundation — delivers the most comprehensive results.
2. While classical cryptography (AES-256, TLS 1.3) is effective against today's threats, the quantum computing threat makes it imperative to urgently introduce post-quantum algorithms (CRYSTALS-Kyber, Dilithium, SPHINCS+). A hybrid approach — operating both in parallel — is the most optimal solution for the transition period.
3. Artificial intelligence — especially federated learning and XAI — transforms cryptographic protection into a dynamic and adaptive system: it enables detection of zero-day vulnerabilities, automation of key management, and transparent auditing.
4. The Republic of Uzbekistan's Decrees PQ-293, PF-37, and PQ-358 lay the groundwork for uniting cryptography, cybersecurity, and AI within a single strategy rather than developing them independently. The proposed four-stage roadmap serves this purpose.
5. The following directions are recommended for future research: creating cybersecurity datasets in the Uzbek language; experimentally measuring the effectiveness of the integration model in the IT Park resident environment; incorporating post-quantum and AI integration requirements into UzDst national standards.

ISSN: 2776-0987 Volume 7, Issue 5, May – 2026

REFERENCES

1. IBM Security. Cost of a Data Breach Report 2024. — New York: IBM Corporation, 2024. [Online]. URL: https://www.ibm.com/reports/data-breach
2. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring // Proceedings 35th Annual Symposium on Foundations of Computer Science. — IEEE, 1994. — P. 124–134.
3. Achuthan K., Ramanathan S., Srinivas S., Raman R. Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions // Frontiers in Big Data. — 2024. — Vol. 7. DOI: 10.3389/fdata.2024.1497535.
4. Presidential Decree No. PQ-293 of the Republic of Uzbekistan "On additional measures for the development of education and science in the field of cryptology in the Republic of Uzbekistan". — Tashkent, August 15, 2024. URL: https://lex.uz/docs/-7067656
5. Presidential Decree No. PQ-358 of the Republic of Uzbekistan "On approval of the strategy for developing artificial intelligence technologies through 2030". — Tashkent, October 14, 2024. URL: https://lex.uz/docs/-7158604
6. Khudoykulov T., Boyquziyev I.M., Allanov O.M., Mardiyev U.R., Jabbarov N.A. Cryptographic Methods: Textbook. — Tashkent: Lesson-Press, 2023. — 255 p.
7. G‘ofurova M.G‘., Tursunova S.A. Application of post-quantum cryptographic algorithms in protecting organizational information systems from quantum threats. // Engineering and Economics. — 2026. — No. 2, special issue (March). — P. 38–43.
8. Khudoyberdiyev O.T. Analysis of modern cryptographic algorithms and their effectiveness // Scientific Bulletin of TUIT named after Muhammad al-Khorazmi. — 2023. — No. 2. — P. 67–74.
9. Karimov N.J. Security mechanisms of the TLS protocol and its practical applications // Problems of Information and Communication Technologies and Telecommunications. — 2022. — No. 1. — P. 101–108.
10. Abdurakhimov B.F., Boyquziyev I.M., Arabboyev A.A. Modern post-quantum cryptographic algorithms and their effectiveness // Al-Farghani Descendants Electronic Scientific Journal. — 2025. — Vol. 1, No. 3. — P. 29–36.
11. G‘ofurova M.G‘. Analysis of modern cryptographic methods for data protection in organizational information systems. // Educational Innovation and Integration. — 2026. — Issue 63, Vol. 1 (February). — P. 287–290. ISSN: 3030-3621. URL: https://journalss.org

ISSN: 2776-0987 Volume 7, Issue 5, May – 2026

12. Bello A.B., Ogundipe A.O., George A.A., Anifowose O. The role of AI and machine learning in cybersecurity: Advancements in threat detection, anomaly detection and automated response // International Journal of Science and Research Archive. — 2025. — Vol. 14, No. 2. — P. 1587–1597. DOI: 10.30574/ijsra.2025.14.2.0542.
13. Arxiv.org. Securing Cryptography in the Age of Quantum Computing and AI: Threats, Defenses, and Protocol Resilience. — 2025. URL: https://arxiv.org/abs/2603.06969
14. Khudoykulov Z., Karimov A., Abdurakhmanov R., Mirzabekov M. Authentication in Cloud Computing: Open Problems // 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC). — IEEE, 2023. DOI: 10.1109/ICESC57686.2023.10193438.
15. G‘ofurova M.G‘. IT Park activities within the framework of the "Uzbekistan – 2030" strategy: export, startup ecosystem and international cooperation. // World Conference on Modern Research Approaches (WCMRA). — April 2026. — P. 8–18. URL: https://imrconf.com/index.php/WCMRA/article/view/2155