

Моя профессиональная
карьера

ISSN

INTERNATIONAL
STANDARD
SERIAL
NUMBER

ISSN

2782-4365

Проверить
номер:



Научно-образовательный электронный журнал

ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ

Выпуск №74-3 (том 2)
(май, 2026)

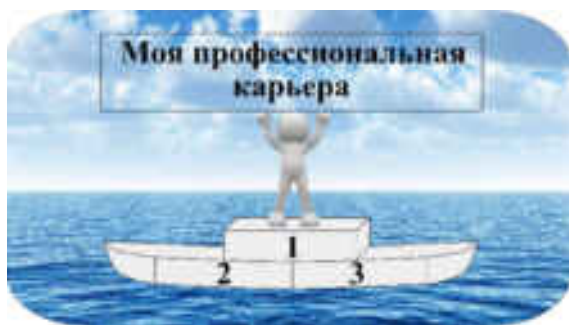


Google
Scholar



Периодичность выпуска: 1 раз в неделю

Сайт: mpcareer.ru/oinv21veke. Почта: obrmppcareer@mail.ru



Международный научно-образовательный
электронный журнал
«ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ»

ISSN 2782-4365

УДК 37

ББК 94

**Международный научно-образовательный электронный журнал
«ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ». Выпуск №74-3 (том 2) (май,
2026). Дата выхода в свет: 18.05.2026.**

Журнал объединяет авторов на территории стран СНГ и помогает обмениваться передовыми научно-образовательными исследованиями.

Содержит научные работы отечественных и зарубежных авторов по экономическим, техническим, философским, юридическим и другим наукам.

Миссия научно-образовательного электронного журнала «ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ» состоит в поддержке интереса читателей к оригинальным исследованиям и инновационным подходам в различных тематических направлениях, которые способствуют распространению лучшей отечественной и зарубежной практики в интернет пространстве.

Целевая аудитория журнала охватывает работников сферы науки и образования (педагоги, учителя, ученые, преподаватели, научные сотрудники, бакалавры, магистранты, аспиранты).

Материалы публикуются в авторской редакции. За соблюдение законов об интеллектуальной собственности и за содержание работ ответственность несут авторы работ. Мнение редакции может не совпадать с мнением авторов научных работ. При использовании и заимствовании материалов ссылка на издание обязательна.

© ООО «МОЯ ПРОФЕССИОНАЛЬНАЯ КАРЬЕРА»

© Коллектив авторов

Allyyev Mekan, Hojamova Lachyn, Bayramov Nurmuhamet STRUCTURAL AND FUNCTIONAL DESIGN OF OPEN CASE 5 STAGE PUMPED WATER PURIFICATION UNIT	158
Mamedov Ahmet, Allagulyyev Begench BLOCKCHAIN-BASED DATA PROTECTION IN DIGITAL INFRASTRUCTURE	167
Annamyradova Selbinyyaz Batyrovna, Yazyyev Erkin Nuryagdyevich BORROWED WORDS IN ENGLISH	171
Агамырат Гельдимырадов Байрамович СОВРЕМЕННЫЕ МЕТОДЫ АНАЛИЗА ЛИПИДОВ В БИОЛОГИЧЕСКИХ СИСТЕМАХ	175
Аннамуратова Гульбахар Гылычмуратовна ОСОБЕННОСТИ ЛИХОРАДОЧНОГО СИНДРОМА ПРИ ВНУТРЕННИХ БОЛЕЗНЯХ	184
Аннамуратова Гульбахар Гылычмуратовна РОЛЬ ТЕЛЕМЕДИЦИНЫ В ТЕРАПЕВТИЧЕСКОЙ ПРАКТИКЕ	189
Реджепова Майса Джумайевна ЗНАЧЕНИЕ И МЕТОДИКА ПРЕПОДАВАНИЯ РУССКОГО ЯЗЫКА ДЛЯ СТУДЕНТОВ МЕДИЦИНСКИХ ВУЗОВ	199
Amanalyyeva Gulshat Batyrovna, Baynazarova Jennet Baynazarovna, Ashyrmuradov Bayrammyrat Ashyrmurat ogly EFFECTIVE STRATEGIES FOR TEACHING VOCABULARY	206
Babajanov Rowshen, Gawirova Oguljan ENERGY-EFFICIENT CYBERSECURITY METHODS FOR IOT SYSTEMS	213
Abduraxmanova Mohichexra Xabib qizi GRAFIK DIZAYNDA SUN'Y INTELLEKT INQILOBI	217
Eziz Kakyshov, Gurbandurdy Tekedurdyyev TECHNOLOGY SELECTION RATIONALE: NEXT.JS, REACT, TYPESCRIPT, SQLITE, AND MATHEMATICAL LIBRARIES	224
Bayramova Nurjemal, Gurbanov Sohbet, Kichigulyyev Gulmyrat, Nuriyev Jelil DEVELOPMENT OF AN AUTONOMOUS SMART VISION ROBOT DESIGNED FOR REAL-TIME HUMAN MOVEMENT TRACKING AND FOLLOWING	229
Atamyrat Altyyev, Ogulkeyik Almazova, Hanova Aynabat POSSIBILITIES OF CREATING HYDROPONIC SYSTEM DEVICE	238
Merdanov Myratmuhammet, Artyklyyev Komekmyrat IMPACT OF VIRTUALIZATION ON DIGITAL INFRASTRUCTURE SECURITY	246

ФИО автора(-ов): *Mamedov Ahmet (student), Allagulyyev Begench (Lecturer)*

Oguz han Engineering and technology University of Turkmenistan (Ashgabat, Turkmenistan)

Название публикации: «BLOCKCHAIN-BASED DATA PROTECTION IN DIGITAL INFRASTRUCTURE»

Annotation: The rapid digitalization of modern infrastructure has significantly increased the volume of sensitive data exchanged across networks, cloud platforms, and distributed systems. As organizations increasingly depend on interconnected digital environments, concerns regarding data integrity, unauthorized access, and cyberattacks continue to grow. Traditional centralized security architectures often suffer from single points of failure, limited transparency, and vulnerability to insider threats. This article introduces and conceptualizes a Blockchain-Based Data Protection System (BBDPS), an intelligent and decentralized framework designed to enhance data security within digital infrastructure environments.

Keywords: blockchain security; digital infrastructure; decentralized systems; data protection; cybersecurity; smart contracts; distributed ledger technology; cryptographic verification.

1. Introduction

The expansion of digital infrastructure has transformed modern society by enabling continuous connectivity across industries such as healthcare, finance, education, transportation, and government services. Organizations increasingly rely on cloud computing, Internet of Things (IoT) devices, distributed databases, and online platforms to store and process massive amounts of sensitive information.

Blockchain technology offers a decentralized alternative for securing digital infrastructure. By distributing records across multiple nodes and using cryptographic consensus mechanisms, blockchain systems provide enhanced transparency, integrity, and resistance against unauthorized modification.

The concept of a Blockchain-Based Data Protection System (BBDPS) aims to address these challenges by integrating decentralized ledger technologies into

cybersecurity frameworks. A BBDPS is defined as a distributed security architecture that stores, validates, and protects digital information through cryptographic consensus, immutable transaction records, and decentralized trust management.

2. Theoretical Foundations

2.1. Blockchain Technology and Distributed Ledgers

Blockchain is a distributed ledger technology that records transactions across multiple interconnected nodes. Each transaction is grouped into blocks that are cryptographically linked to previous blocks, creating an immutable chain of records.

Consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT) ensure that all nodes agree on the validity of transactions before new records are added to the blockchain.

2.2. Cryptographic Data Protection

Cryptography forms the foundation of blockchain security. Blockchain systems utilize hashing algorithms, digital signatures, and asymmetric encryption to protect data integrity and verify transaction authenticity.

Hash functions generate unique digital fingerprints for each block of data. Even a minor modification to stored information changes the hash value, immediately revealing tampering attempts.

2.3. Decentralized Trust and Smart Contracts

Traditional digital infrastructures rely on centralized authorities to establish trust between participants. Blockchain systems replace centralized trust with decentralized consensus mechanisms that validate actions transparently across the network.

Smart contracts extend blockchain functionality by automating security policies and operational procedures. These self-executing programs automatically enforce predefined conditions without requiring human intervention.

3. Benefits and Challenges

3.1. Benefits

1. **Enhanced data integrity:** Immutable blockchain records significantly reduce the risk of unauthorized data modification.

2. **Decentralized security:** Removing centralized control points minimizes vulnerabilities associated with single points of failure.
3. **Improved transparency and traceability:** Every transaction is permanently recorded and auditable, increasing accountability.
4. **Automated protection mechanisms:** Smart contracts enable real-time enforcement of security policies without manual intervention.

3.2. Challenges

1. **Scalability limitations:** Blockchain systems may experience performance bottlenecks when processing large volumes of transactions.
2. **Energy consumption:** Some consensus mechanisms, particularly Proof of Work, require substantial computational resources.
3. **Regulatory and legal concerns:** Data privacy regulations may conflict with the immutable nature of blockchain records.
4. **Integration complexity:** Incorporating blockchain technologies into existing infrastructure can require significant technical and organizational changes.

4. Future Research Directions

1. **AI-enhanced blockchain security:** Combining artificial intelligence with blockchain systems to improve anomaly detection and predictive cybersecurity capabilities.
2. **Energy-efficient consensus mechanisms:** Developing sustainable alternatives to energy-intensive blockchain validation methods.
3. **Quantum-resistant cryptography:** Designing blockchain encryption techniques capable of resisting future quantum computing threats.
4. **Cross-chain interoperability:** Enabling secure communication and data exchange between multiple blockchain networks.
5. **Decentralized identity management:** Building blockchain-based identity frameworks that provide users with greater control over personal data and authentication processes.

5. Conclusion

Blockchain-Based Data Protection Systems represent a transformative approach to securing modern digital infrastructure. By combining decentralized ledger technology, cryptographic verification, and automated smart contract enforcement, BBDPS frameworks offer enhanced resilience against cyberattacks, unauthorized modifications, and centralized system failures.

Future research should focus on improving interoperability, optimizing performance, and integrating intelligent threat detection systems capable of adapting to rapidly evolving cyber threats.

References

1. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
2. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation Review*, 2, 6–19.
3. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access*, 4, 2292–2303.
4. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *IEEE International Congress on Big Data*, 557–564.
5. Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Blockchain in internet of things: Challenges and solutions. *arXiv preprint arXiv:1608.05187*.
6. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications. *Telematics and Informatics*, 36, 55–81.