

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)

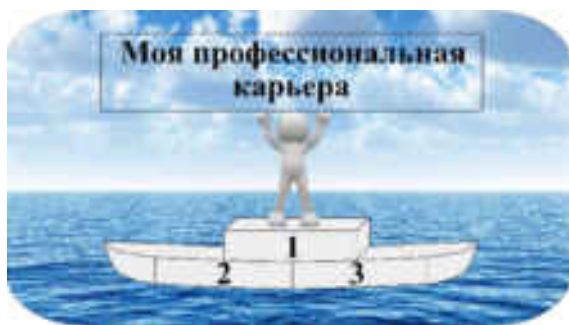


Google
Scholar



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

Chakkanov Rustem, Gawirova Oguljan INTERSECTION OF DATA SCIENCE AND CYBERSECURITY IN DIGITAL INFRASTRUCTURE	250
Eziz Myratberdi, Bayramdurdyev Serdar JWT TOKEN ATTACKS AND DEFENSES	255
S.Xashimov, O'.N.Ikromov MAHALLA AHOLISI SOG'LIQ HOLATINI MONITORING QILISH AXBOROT TIZIMINI ISHLAB CHIQISH	259
Nortajiyeva Ra'no Nurmatovna HAYOT GO'ZAL — YASHASH UCHUN 1001 SABAB	268
Dovlatov Shoxzod Shuxrat o'g'li 35 kV DAN YUQORI KUCHLANISHLI ELEKTR TARMOQLARIDA ENERGIYA YO'QOTISHLARINI KAMAYTIRISH USULLARINI TAKOMILLASHTIRISH	272
Meredova Mahri THE IMPACT OF SOCIAL MEDIA ON MODERN GERMAN SLANG	278
Meredova Mahri THE POWER OF IMMERSION: HOW TO THINK IN ENGLISH, NOT JUST TRANSLATE	285
Meredova Mahri ENGLISH FOR SPECIFIC PURPOSES (ESP): BEYOND BASIC COMMUNICATION	292
Meredova Mahri, Charyev Hemra, Meredova Akmaral UNCONVENTIONAL RENEWABLE ENERGY SOURCES: THE FRONTIERS OF FUTURE POWER GENERATION	299
Annamyradov Yhlasmuhammet, Gawirova Oguljan MULTI-TENANCY SECURITY IN CLOUD SYSTEM	305
Igdyrova Patma, Atamyrat Altyev, Myradova Tumar INNOVATIVE METHODS OF INTERACTION OF VARIOUS SUBSTANCES USED IN THE SYNTHESIS OF ULTRAMARINE	308
Abdylov Eziz, Gylyjov Annamyrat NETWORK QUALITY MONITORING SYSTEM	313
Suhrapova Nurjahan, Allagulyev Begench CLOUD NETWORK DATA PROTECTION PROTOCOLS	319
Ogulkeyik Almazova, Atamyrat Altyev, Oguldondi Satymova TECHNOLOGY FOR OBTAINING SAPONINS FROM ALHAGI MAURORUM AND THEIR POTENTIAL APPLICATIONS	329
Orazdurdyev Aymyrat, Babalakov Azym, Akmuradova Sulgun, Annachyev Yhlas AQUA-TECH FILTRATION SYSTEM	334
Narzullayev Serdar, Bayramdurdyev Serdar PASSWORD HASH ATTACK SIMULATOR	339

ФИО автора(-ов): *Chakkanov Rustem (student), Gawirova Oguljan (Lecturer)*
Oguz han Engineering and technology University of Turkmenistan (Ashgabat, Turkmenistan)

Название публикации: «INTERSECTION OF DATA SCIENCE AND CYBERSECURITY IN DIGITAL INFRASTRUCTURE»

Annotation: The rapid evolution of digital infrastructure has led to an unprecedented increase in data generation, interconnected systems, and cybersecurity threats. Organizations operating in sectors such as finance, healthcare, transportation, and cloud computing increasingly depend on large-scale digital ecosystems that require advanced protection mechanisms. Traditional cybersecurity approaches often struggle to detect sophisticated attacks due to the growing complexity and volume of network activity. This article introduces and conceptualizes the integration of Data Science and Cybersecurity (DSC) as an intelligent framework for enhancing digital infrastructure protection. Unlike conventional rule-based security systems, DSC combines machine learning, big data analytics, anomaly detection, and predictive modeling to identify, analyze, and mitigate cyber threats in real time.

Keywords: data science; cybersecurity; digital infrastructure; machine learning; threat detection; anomaly analysis; predictive security; big data analytics.

1. Introduction

Digital infrastructure has become the foundation of modern society, supporting communication systems, cloud platforms, e-commerce, healthcare services, financial transactions, and smart city technologies. As organizations continue to adopt interconnected digital environments, the amount of generated data has increased dramatically.

At the same time, cyber threats have become more advanced, automated, and difficult to detect using traditional security approaches. Attackers increasingly exploit artificial intelligence, automation tools, and large-scale attack networks to compromise digital systems. Conventional cybersecurity systems that rely primarily on static rules

and signature-based detection often fail to identify previously unseen threats or rapidly evolving attack patterns.

2. Theoretical Foundations

2.1. Data Science and Big Data Analytics

Data science focuses on extracting meaningful insights from structured and unstructured data through statistical analysis, machine learning, and computational techniques. In digital infrastructure environments, massive volumes of data are generated through network traffic, authentication logs, cloud services, IoT devices, and user interactions.

2.2. Machine Learning in Cybersecurity

Machine learning algorithms enable cybersecurity systems to learn from historical data and identify abnormal behavior patterns automatically. Unlike traditional signature-based systems, machine learning models can detect previously unknown threats by analyzing deviations from normal activity.

Supervised learning models can classify malware, phishing attempts, and malicious network traffic, while unsupervised learning techniques are effective for anomaly detection in environments where attack signatures are unavailable.

3. Practical Applications

3.1. Intrusion Detection Systems

A DSC framework can monitor network traffic in real time and identify suspicious activities such as unauthorized access attempts, malware propagation, or abnormal communication patterns.

Machine learning algorithms can analyze traffic behavior and distinguish between legitimate users and malicious actors more effectively than traditional rule-based systems.

3.2. Fraud Detection in Financial Systems

Financial institutions generate large amounts of transaction data that can be analyzed to detect fraudulent activities. Data science models can identify unusual transaction behavior, unauthorized account access, or abnormal spending patterns.

Predictive analytics can also estimate fraud probability and automatically trigger additional authentication procedures or temporary transaction restrictions.

4. Benefits and Challenges

4.1. Benefits

1. **Improved threat detection:** Intelligent analytical systems can identify complex and previously unknown cyber threats.
2. **Real-time cybersecurity monitoring:** Large-scale data processing enables continuous infrastructure surveillance.
3. **Predictive defense capabilities:** Organizations can anticipate threats and apply preventive measures before attacks occur.
4. **Automation of security operations:** Data-driven systems reduce manual workload for cybersecurity analysts and improve response efficiency.

4.2. Challenges

1. **Data privacy concerns:** Collecting and analyzing large volumes of user and infrastructure data raises ethical and legal issues.
2. **High computational requirements:** Advanced machine learning and big data processing demand significant computing resources.
3. **False positives and model accuracy:** Machine learning systems may incorrectly classify legitimate behavior as malicious.
4. **Adversarial AI threats:** Attackers may attempt to manipulate or evade machine learning models through adversarial techniques.

5. Future Research Directions

1. **Explainable AI in cybersecurity:** Developing transparent machine learning models that allow analysts to understand automated threat detection decisions.
2. **Federated cybersecurity learning:** Enabling collaborative threat intelligence sharing without exposing sensitive organizational data.

3. **Quantum-enhanced cybersecurity analytics:** Investigating quantum computing techniques for advanced threat analysis and encryption security.
4. **Autonomous cyber defense systems:** Designing fully automated security architectures capable of independent threat response and adaptation.

6. Conclusion

The intersection of Data Science and Cybersecurity represents a transformative approach to protecting modern digital infrastructure. By integrating machine learning, big data analytics, behavioral analysis, and predictive modeling, DSC frameworks provide intelligent and adaptive defense mechanisms against increasingly sophisticated cyber threats.

As digital ecosystems continue to expand, organizations will require cybersecurity systems capable of processing vast amounts of information in real time while continuously adapting to evolving attack strategies. Although challenges related to privacy, computational complexity, and model reliability remain significant, data-driven cybersecurity offers substantial opportunities for improving resilience and operational security.

Future advancements in artificial intelligence, predictive analytics, and autonomous defense technologies are expected to further strengthen the role of data science in securing digital infrastructure environments.

References

1. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*, 305–316.
2. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.
3. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.

4. Shafiq, M., Tian, Z., Bashir, A. K., Du, X., & Guizani, M. (2020). Corrauc: A malicious bot-IoT traffic detection method in IoT network using machine-learning techniques. *IEEE Internet of Things Journal*, 8(5), 3242–3254.