

# INNOVATION SCIENCE AND TECHNOLOGY

**ISSUE 6, PART 1 / JUNE 2026**

 Acceptance of papers



**Acceptance of  
papers**

Published monthly



**Topics**

economics,  
technology, social  
sciences



**EDITOR-IN-CHIEF:**

Mirzaliyev Sanjar Makhmatjon ugli

**DEPUTY EDITOR-IN-CHIEF:**

Makhmudov Nosir Makhmudovich  
DSc., Prof., Academician

**DEPUTY EDITOR-IN-CHIEF:**

Ochilov Bobur Bakhtiyor ugli – Senior  
lecturer at TSUI

THE SCIENTIFIC-POPULAR ELECTRONIC  
JOURNAL **"INNOVATION SCIENCE AND  
TECHNOLOGY"** HAS BEEN REGISTERED  
UNDER THE NUMBER **C-5669633** BY THE  
AGENCY FOR INFORMATION AND MASS  
COMMUNICATIONS (AOKA) OF THE  
REPUBLIC OF UZBEKISTAN, EFFECTIVE  
FROM OCTOBER 9, 2024.

**CONTACTS**

Phone: **+998 50 737 87 88**

Website: <https://ist-journal.uz>

Email: [innovationist2025@gmail.com](mailto:innovationist2025@gmail.com)

The scientific electronic journal "Innovation Science and Technology" has been included in the list of scientific publications recommended for the publication of main scientific results of dissertations for the award of PhD and DSc degrees in economics and technical sciences, in accordance with the Resolution No. 370 of the Presidium of the Higher Attestation Commission of the Republic of Uzbekistan, dated May 8, 2025.

**Editorial board:**



**Sharipov Kongiratbay Avezimbetovich,**  
Doctor of Technical Sciences (DSc), Professor



**Abdurakhmanova Gulnora Kalandarovna,** Doctor of  
Economic Sciences (DSc), Professor



**Cham Tat Huei,**  
Doctor of Philosophy (PhD), Professor (Malaysia)



**Muhammad Imran Sadiq**  
Doctor of Philosophy in Economics (PhD), Professor,  
Malaysia



**Ahmed Aziz Ismail**  
Doctor of Technical Sciences (DSc),  
Professor (Egypt)



**Lee Chin**  
Doctor of Philosophy in Economics (PhD), (Malaysia)



**Asongu Simplice**  
Doctor of Philosophy in Economics (PhD), Cameroon



**Rui Dang**  
Doctor of Chemistry (DSc), Professor, China



**Zahoor Ahmed**  
Doctor of Philosophy in Economics (PhD), Turkey



**Shujaat Abbas**  
Doctor of Philosophy in Economics (PhD), Russia



**Tina A Coffelt**  
Doctor of Philosophy in Educational Sciences (PhD),  
USA



**Abdikarimova Dinara Rustamxanovna**  
Doctor of Economic Sciences (DSc), Professor

**Kurbonbekova Mohichehra Turobjonovna**  
Doctor of Economic Sciences (DSc), Professor

**Alimardonov Ilkhom Muzrabshokovich**  
Doctor of Economic Sciences (DSc), Professor



**Razakova Barno Sayfieva**  
Doctor of Philosophy in Economics (PhD)



**Khasanov Sarvar Ulugbek ugli**  
Doctor of Philosophy in Economics (PhD)



**Kholikova Rukhsora Sanjarovna**  
Associate Professor (PhD)

# CONTENTS

|                                                                                                                     |    |
|---------------------------------------------------------------------------------------------------------------------|----|
| BUDGETING BASED ON THE BALANCED SCORECARD SYSTEM IN STRATEGIC MANAGEMENT ACCOUNTING.....                            | 8  |
| <b>Pardaeva Shakhnoza Abdinabievna</b>                                                                              |    |
| TURIZM SOHASIDA TARJIMA NAZARIYASINING O'RNI .....                                                                  | 13 |
| <b>Bahronova Charos Mirabbos qizi</b>                                                                               |    |
| THE ROLE OF ESG PRINCIPLES AND DIGITAL TECHNOLOGIES IN THE DEVELOPMENT OF CORPORATE SOCIAL MANAGEMENT SYSTEMS ..... | 16 |
| <b>Shokhrukh Abdisalimovich Muratkosimov</b>                                                                        |    |
| A COMPARATIVE SEMANTIC FIELD ANALYSIS OF "BENEFIT" ACROSS ENGLISH AND UZBEK CULTURES .....                          | 23 |
| <b>Mohira Husanovna Divanova</b>                                                                                    |    |
| ROSSIYA TIJORAT BANKLARIDA DEPOZIT OPERATSIYALARINI RIVOJLANTIRISHNING O'ZIGA XOS JIHATLARI .....                   | 30 |
| <b>Rahimov Akmal Matyaqubovich</b>                                                                                  |    |
| USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES AGAINST CYBER THREATS IN THE PUBLIC SECTOR.....                         | 37 |
| <b>Nuratdinov Xushnid Begzadovich, Erejepov Kewlimjay Kaymatdinovich</b>                                            |    |

# USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES AGAINST CYBER THREATS IN THE PUBLIC SECTOR

**Nuratdinov Xushnid Begzadovich**

Student of Nukus State Technical University

E-mail: [husnidnuratdinov@gmail.com](mailto:husnidnuratdinov@gmail.com)

**Erejepov Kewlimjay Kaymatdinovich**

Associate Professor of the Department of Computer

Engineering, Nukus State Technical University, PhD in Technical Sciences

E-mail: [k.erejepov@nukusstu.uz](mailto:k.erejepov@nukusstu.uz)

ORCID: 0009-00040413-5428

**Abstract.** The article addresses the application of artificial intelligence and machine learning technologies for protecting public-sector information systems against cyber threats. The inadequacy of classical signature-based tools against modern attacks is analyzed. The use of ML models for intrusion detection, malware classification, phishing protection, and user behavior analytics is reviewed. New risks linked to the use of AI tools by attackers themselves are discussed.

**Keywords:** artificial intelligence, cybersecurity, public sector, machine learning, intrusion detection, phishing, deepfake.

**Annotatsiya.** Maqolada davlat sektorining axborot tizimlarini kibertahdidlardan himoya qilishda sun'iy intellekt va mashinali o'qitish texnologiyalaridan foydalanish masalalari ko'rib chiqilgan. Klassik imzoga asoslangan vositalarning zamonaviy hujumlar oldida samarasizligi tahlil qilingan. ML-modellarining hujumlarni aniqlash, zararli dasturlarni tasniflash, fishingga qarshi himoya va xulq-atvor tahlilida qo'llanilishi yoritilgan. Hujumchilar tomonidan SI vositalaridan foydalanish bilan bog'liq yangi xavflar tahlil qilingan.

**Kalit so'zlar:** sun'iy intellekt, kiberxavfsizlik, davlat sektori, mashinali o'qitish, hujumlarni aniqlash, fishing, deepfake.

**Аннотация.** В статье рассмотрены вопросы применения искусственного интеллекта и машинного обучения для защиты информационных систем государственного сектора от киберугроз. Проанализирована недостаточность классических сигнатурных средств перед современными атаками. Освещено использование ML-моделей в задачах обнаружения вторжений, классификации вредоносного ПО, защиты от фишинга и анализа поведения пользователей. Проанализированы новые риски, связанные с использованием инструментов ИИ самими злоумышленниками.

**Ключевые слова:** искусственный интеллект, кибербезопасность, государственный сектор, машинное обучение, обнаружение атак, фишинг, дипфейк.

## INTRODUCTION

Over the last ten years, the informatization of the public sector has accelerated sharply: public services have moved to electronic platforms, citizens' data are being stored in cloud repositories, and interagency communication is being carried out through digital channels. Within the framework of the "Digital Uzbekistan – 2030" Strategy, this process has accelerated even further. However, along with the expansion of digital infrastructure, the number and complexity of attacks directed at public information resources are also increasing [1]. Figure 1 presents the growth dynamics of cyberattacks targeting the public sector during 2019–2024.

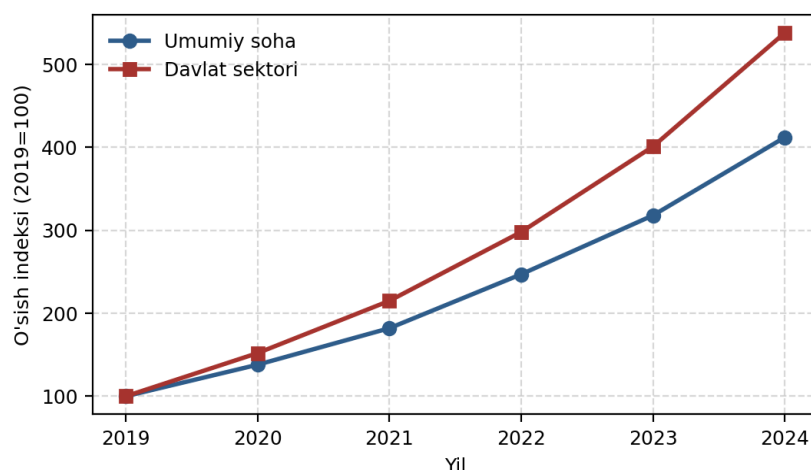


Figure 1. Dynamics of Cyberattack Growth (2019–2024)

Traditional security tools—signature-based antivirus software, static firewalls, and rule-based IDS—were designed for a closed and previously known threat model. Polymorphic malware rewrites its code each time it is executed, fileless attacks exist only in volatile memory, and zero-day attacks have no signatures at all [2]. Machine Learning (ML) learns from historical data and generalizes to previously unseen samples, making it possible to detect attacks without predefined rules [3]. The purpose of this article is to systematically review the application of AI technologies in combating cyber threats in the public sector and to analyze the associated risks.

## LITERATURE REVIEW

The integration of artificial intelligence and cybersecurity has become one of the important directions of scientific research in recent years. As digital transformation processes accelerate, the issue of protecting information systems in the public sector is gaining increasing importance. For this reason, many researchers are paying special attention to studying the capabilities of artificial intelligence and machine learning technologies in cybersecurity.

One of the early scientific studies on the application of machine learning methods in cybersecurity was conducted by Sommer and Paxson, who analyzed the advantages and limitations of machine learning in anomaly detection systems. The researchers emphasize that the constantly evolving nature of cyberattacks reduces the effectiveness of traditional signature-based security tools, thereby increasing the need for adaptive intelligent systems.

Buczak and Guven conducted a comprehensive analysis of the application of machine learning algorithms in cybersecurity and demonstrated the effectiveness of supervised and unsupervised learning methods in attack detection. According to the authors, Random Forest, Support Vector Machine, and Decision Tree algorithms provide high performance in detecting network attacks.

The deep learning theory developed by Goodfellow, Bengio, and Courville was later introduced into cybersecurity systems. The effectiveness of CNN and LSTM models in network traffic analysis, malware detection, and user behavior monitoring has been confirmed by numerous studies. Research conducted by Kim and colleagues showed that deep neural networks achieve higher accuracy in malware detection compared to traditional approaches.

Studies by Sarker, Alazab, and Mahmood on the impact of artificial intelligence on cybersecurity in the public sector highlight the advantages of intelligent threat detection mechanisms for public information systems. The authors emphasize that AI technologies make it possible to conduct real-time monitoring, predict threats, and automatically analyze security incidents.

In recent years, scientific literature has also paid increasing attention to the negative aspects of artificial intelligence. Huang, Kwon, and other researchers have examined adversarial machine learning issues and demonstrated the risks of poisoning and evasion attacks against machine learning models. In addition, it has been noted that generative artificial intelligence and large language models (LLMs) enable the creation of phishing emails, deepfake audio, and video materials, thereby increasing the sophistication of cybercriminal activities.

The analyzed scientific sources indicate that artificial intelligence technologies are a promising tool for

ensuring cybersecurity in the public sector. However, when implementing them in practice, it is also necessary to consider factors such as data privacy, model transparency, resilience to adversarial attacks, and legal-regulatory requirements.

## RESEARCH METHODOLOGY

This study was conducted as a theoretical-analytical investigation aimed at analyzing the possibilities of using artificial intelligence technologies in combating cyber threats in the public sector. During the research process, scientific literature, reports of international organizations, and contemporary applied studies related to cybersecurity, artificial intelligence, and machine learning were examined.

The theoretical foundation of the study was formed by scientific concepts related to artificial intelligence, machine learning, deep learning, and cybersecurity. In particular, modern approaches to cyberattack detection, malware classification, phishing prevention, user behavior analysis, and network security were analyzed.

Comparative-analytical, system analysis, content analysis, and generalization methods were employed in the study. The comparative-analytical method was used to compare the advantages and disadvantages of traditional cybersecurity tools and AI-based protection systems. Through system analysis, the relationship between major cyber threats in the public sector and the AI technologies used to counter them was examined. Content analysis was applied to scientific articles, technical reports, and international practices in order to identify current trends and challenges.

The data sources included Scopus, Web of Science, IEEE Xplore, Springer, Elsevier, Google Scholar, and open reports published by international cybersecurity organizations. In addition, recent studies related to public information system security, adversarial machine learning, deepfake technologies, and large language models were reviewed.

Logical generalization and scientific synthesis methods were used to process and analyze the collected information. Based on the research findings, scientific conclusions were formulated regarding the advantages, existing limitations, and prospective development directions of the use of artificial intelligence technologies in the public sector.

## RESULTS AND ANALYSIS

The composition of threats targeting the public sector differs from that of the private sector. Figure 2 presents the distribution of the main types of attacks: phishing and ransomware occupy the leading positions, while APT groups and insider threats also represent a significant share.

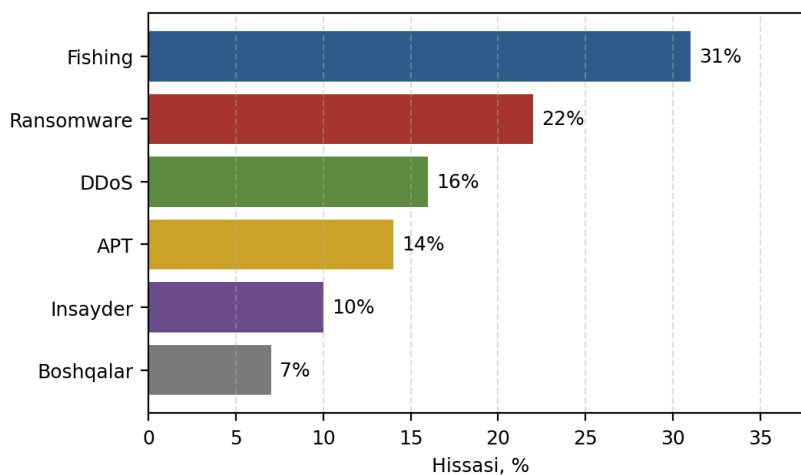


Figure 2. Shares of Cyber Threat Types Targeting the Public Sector

In practice, the main AI approaches are as follows: supervised learning (logistic regression, Random Forest, XGBoost) works with labeled data and provides high accuracy in classifying spam, phishing, and malware [4]; unsupervised learning (isolation forest, autoencoders) does not require labeling and detects anomalies, including zero-day attacks [5]; deep learning (CNN, LSTM, transformers) operates on raw traffic and sequences of system calls but requires significant computational resources [6]; NLP and large language models (LLMs) extract meaning from emails and log records, helping to prioritize alerts and prepare reports in Security Operations Centers (SOCs) [7].

In the public sector, these methods are applied in several key areas. Intrusion Detection Systems (IDS/

NIDS) operate using a hybrid architecture: a signature engine is used for known attacks, while the ML anomaly layer is responsible for zero-day attacks and APT activity. APT groups often remain hidden within a network for weeks or even months, and unsupervised methods are necessary to detect their lateral movement. In malware analysis, static features (opcode frequencies, imported APIs, section entropy) and dynamic sandbox analysis are combined—the former performs preliminary filtering, while the latter confirms the results [8]. The classification of ransomware families deserves special attention: models identify new strains through behavioral similarity with previously known families. In phishing protection, NLP detects social engineering patterns (urgency, authority impersonation, unusual wording), while computer vision compares screenshots of suspicious websites with templates to detect visual imitation [9]. UEBA systems build normal behavioral profiles for each user and device and detect insider threats, including employee misuse and account compromise following password leaks [10]. At the SOC level, ML prioritizes and correlates alerts: the average SIEM in a government organization generates tens of thousands of events per day, and without ML methods analysts would be unable to investigate most of them. Deep learning methods (CNN, LSTM) demonstrate higher accuracy and lower false-positive rates compared to classical signature-based IDS systems: several empirical studies have reported accuracy above 96% for CNN models, while false-positive rates remained below 3%.

Adversarial machine learning (adversarial ML) has emerged as an independent field of study. Evasion attacks identify input data that cause a classifier to produce incorrect results, such as malware disguised as benign software or images altered with imperceptible noise. Poisoning attacks insert contaminated samples into training datasets and establish backdoors that can be activated by specific triggers [11]. If a model makes security-related decisions in production environments, it will eventually be tested by attackers.

Attackers have also adopted AI into their arsenal. By using LLMs, it is possible to create well-written phishing messages in various languages—including Uzbek and Russian—and the old rule of “poor spelling means a suspicious email” no longer applies. Deepfake voice technology has already been used in real fraud cases: a subordinate employee was called using a manager’s voice and persuaded to authorize a money transfer [12]. This threat is particularly acute in the public sector, where decisions are often made on the basis of voice or video confirmation.

Data and interpretability issues also remain significant. Attacks are relatively rare, while normal traffic exists in large volumes, meaning that classes may be imbalanced by hundreds of times. Regulations governing the processing of personal data impose substantial restrictions on the generalization of data for model training, and data sharing between organizations is often legally prohibited. In addition, analysts must understand why a model generated an alert; without such information, it is impossible to justify decisions to management. SHAP and LIME methods provide partial solutions, but the trade-off between accuracy and interpretability remains an open issue [13].

## CONCLUSION AND RECOMMENDATIONS

Artificial intelligence is becoming firmly established within the cybersecurity systems of the public sector. In SOCs, ML removes part of the analysts’ repetitive workload; in IDS systems, it detects attacks for which no signatures have been written; and in UEBA systems, it identifies insider threats. At the same time, AI has introduced new risks: models can be attacked, deceived, and stolen, while attackers themselves are increasingly making effective use of generative tools. The specific characteristics of the public sector—data confidentiality, requirements for transparency in decision-making processes, and legal constraints—require AI implementation to be carried out more cautiously than in the private sector. AI has not become a “silver bullet”; rather, it is a working tool, and its value depends on how carefully it is applied, how clean the input data are, and how critically people evaluate its outputs.

## LIST OF REFERENCES

1. ENISA. ENISA Threat Landscape 2023. - European Union Agency for Cybersecurity, 2023. - 144 p.
2. Saranya T., Sridevi S., Deisy C. et al. Performance analysis of machine learning algorithms in intrusion detection system: A review // *Procedia Computer Science*. - Elsevier, 2020. - Vol. 171. - P. 1251-1260.
3. Sarker I. H., Kayes A. S. M., Badsha S. et al. Cybersecurity data science: an overview from machine learning perspective // *Journal of Big Data*. - Springer, 2020. - Vol. 7, No. 41. - P. 1-29.
4. Buczak A. L., Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection // *IEEE Communications Surveys & Tutorials*. - IEEE, 2016. - Vol. 18, No. 2. - P. 1153-1176.
5. Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey // *ACM Computing Surveys*. - ACM, 2009. - Vol. 41, No. 3. - P. 1-58.
6. Xin Y., Kong L., Liu Z. et al. Machine learning and deep learning methods for cybersecurity // *IEEE Access*. - IEEE, 2018. - Vol. 6. - P. 35365-35381.

7. Perez F., Ribeiro I. Ignore previous prompt: Attack techniques for language models // NeurIPS ML Safety Workshop, 2022. - P. 1-10.
8. Ucci D., Aniello L., Baldoni R. Survey of machine learning techniques for malware analysis // Computers & Security. - Elsevier, 2019. - Vol. 81. - P. 123-147.
9. Jain A. K., Gupta B. B. A survey of phishing attack techniques, defense mechanisms and open research challenges // Enterprise Information Systems. - Taylor & Francis, 2022. - Vol. 16, No. 4. - P. 527-565.
10. Salem M., Hershkop S., Stolfo S. J. A survey of insider attack detection research // Insider Attack and Cyber Security. - Springer, 2008. - P. 69-90.
11. Biggio B., Roli F. Wild patterns: Ten years after the rise of adversarial machine learning // Pattern Recognition. - Elsevier, 2018. - Vol. 84. - P. 317-331.
12. Mirsky Y., Demontis A., Kotak J. et al. The threat of offensive AI to organizations // Computers & Security. - Elsevier, 2023. - Vol. 124. - P. 1-28.
13. Arrieta A. B., Diaz-Rodriguez N., Del Ser J. et al. Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI // Information Fusion. - Elsevier, 2020. - Vol. 58. - P. 82-115.

**Proofreader:** Zokir ALIBEKOV  
**Layout and Designer:** Oloviddin Sobir ugli

---

## 2026. № 6

---

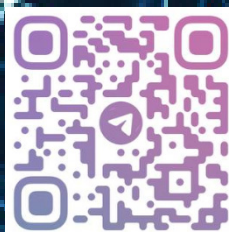
© When materials are reproduced, the INNOVATION SCIENCE AND TECHNOLOGY journal must be cited as the source. Authors are responsible for the accuracy of the information in materials and advertisements published in the journal. Editorial opinions may not always align with those of the authors. Submitted materials will not be returned to the editorial office.

To publish articles in this journal, you may submit articles, advertisements, stories, and other creative materials through the following links. Materials and advertisements are published on a paid basis.

You may subscribe to the journal at any time using the following details. Once subscribed, please send a screenshot or photo of your payment confirmation to our Telegram page @iqtisodiyot\_77. Based on this, we will send the latest issue of the journal to your address each month.

“The journal “INNOVATION SCIENCE AND TECHNOLOGY” has been registered by the Agency for Information and Mass Communications under the Administration of the President of the Republic of Uzbekistan from 09.10.2024 under the registration number №390637. License number: C-5669633. PNFL: 30407832680027

**Our address:** Tashkent city, Yunusobod district, 19th block,  
House 17.



### Acceptance of articles

Published every  
monthly



### Directions

Social, economic, political,  
technological, scientific



**Scopus** || Scientific electronic journal specializing in Scopus

**CERTIFICATE NUMBER: №390637**

**ORDER NUMBER ACCORDING TO  
THE LICENSE REGISTER: C-5669633**

### CONTACT:



Contact us  
**+998 50 737 87 88**



Telegram channel  
**t.me/scopus\_IST2100**



Journal official website  
<https://ist-journal.uz/index.php/IST>