



Central Asian  
Scientific  
Journal

**VOL 1(29)  
2026**



**ASTANA**

Электронный научный журнал «Central Asian Scientific Journal»

# Central Asian Scientific Journal

выпуск №1 (29), январь – март 2026 г.  
Том 2

Основан в 2021 году (издается ежеквартально)

зарегистрирован в Комитете информации Министерства  
информации и общественного развития Республики  
Казахстан №KZ40VPY00067791 от 07.04.2023 г.

## Тақырыптық бағыт:

- Pedagogikalyq, qoǵamdyq-áleýmettik, tehnikalyq, ekonomikalyq jáne zań ǵylymdary
- Aqparattyq-komúnikasıalyq tehnologıalar
- Teorialyq jáne ǵylymı-praktıkalyq ǵylymı zertteýler

## Тематическая направленность:

- Педагогические, общественно-социальные, технические, экономические и юридические науки
- Информационно-коммуникационные технологии
- Теоретические и научно-практические научные исследования

## Thematic focus:

- Pedagogical, socio-political, technical, economic, and legal sciences
- Information and communication technologies
- Theoretical and scientific-practical research

*Jarıalanatyn aqparattyń, dáıeksózderdiń jáne ózge de baıandamalaryń durıstyǵy úshin avtor jaýapty bolady*

*За достоверность публикуемой информации, цитат и иных изложений ответственность несет автор*

*The author is responsible for the accuracy of the published information, quotes, and other statements.*



"Central Asian Scientific  
Journal" elektronдық ғылыми  
журналы аппараты  
agenttigi

Информационное агентство  
Электронный научный журнал  
«Central Asian Scientific  
Journal»

Information Agency Electronic  
scientific Journal "Central Asian  
Scientific Journal"

№1 (29), 2026 j  
Shyǵarý jiligi – jylyna 4 nómir  
2021 j. bastap shyǵady

№1 (29), 2026 г.  
Периодичность – 4 номера в год  
Выходит с 2021 года

No.1 (29), 2026  
Periodicity: 4 issues per year  
Since 2021

Bas redaktor:  
Baidildinov T. J. – p. ǵ. k.,  
professor

Главный редактор:  
Байдильдинов Т.Ж. – к.п.н.,  
профессор

Editor-in-Chief:  
Baidildinov T.Zh. – Ph.D.,  
Professor

Redaksialyq alqa:  
Latypov R.H. – t. ǵ. d.,  
prof., Qazan, Resei  
Radwan Labban –  
Plymouth College, United  
Kingdom  
Safarov G.A. – e. ǵ. d.,  
prof., Tashkent, Ózbekstan  
Mýkasheva A.A. – z.ǵ. d.,  
prof., L.N. Gýmilev  
atyndaǵy EÝU  
Baǵojanova D.S. – p. ǵ. k.,  
HAA akademigi  
Kojasheva G.O. – p.ǵ.  
k., docent, Abay atyndaǵy  
KazPÝU  
Teleýev G.B. – PhD, QAÝ  
Ózdenbaev J.Ş. – t. ǵ. k.,  
I.Jansügirov atyndaǵy JU  
Nürǵaliev S.A. – PhD,  
asistent professor, AITU

Редакционная коллегия:  
Латыпов Р.Х. – д.т.н., проф.,  
Казань, Россия  
Radwan Labban – Plymouth  
College, United Kingdom  
Сафаров Г.А. – д.э.н., проф.,  
Ташкент, Узбекистан  
Мукашева А.А. – д.ю.н., проф.,  
ЕНУ им. Л.Н. Гумилева  
Байгожанова Д.С. – к.п.н.,  
академик МАИН  
Кожашева Г.О. – к.п.н, доцент,  
КазНПУ им. Абая  
Телеуев Г.Б. – PhD, KAU  
Узденбаев Ж.Ш. – к.т.н.,  
ст.преподаватель, ЖУ им.  
И.Жансугурова  
Нургалиева С.А. – PhD,  
ассистент.проф., AITU

Editorial Board:  
Latypov R.H. – Doctor of  
Technical Sciences, Professor,  
Kazan, Russia  
Radwan Labban – Plymouth  
College, United Kingdom  
Safarov G.A. – Doctor of  
Economic Sciences, Professor,,  
Tashkent, Uzbekistan  
Mukasheva A.A. – Doctor of Law,  
Professor, L.N. Gumilyov ENU  
Baigozhanova D.S. – Ph.D.,  
Academician of the MAIN  
Kozhasheva G.O. – c.p.s, Abay  
KazNPU  
Teleuev G.B. – PhD, KAU  
Uzdenbaev Zh.Sh. – Candidate  
of Technical Sciences,  
Zhansugurov ZhU  
Nurgaliyeva S.A. – PhD, assistant  
prof., AITU

Qazaqstan Respýblıkasy  
Aqparat jáne qoǵamdyq  
damý ministrliginiń  
07.04.2023 j.  
№KZ40VPY00067791  
aqparat komitetinde  
tirkelgen.

Зарегистрирован в Комитете  
информации Министерства  
информации и  
общественного развития  
Республики Казахстан  
№KZ40VPY00067791 от  
07.04.2023

Registered with the Information  
Committee of the Ministry of  
Information and Public  
Development of the Republic of  
Kazakhstan No.  
KZ40VPY00067791 dated  
07.04.2023.

JK DOC, 010000,  
Qazaqstan Respýblıkasy,  
Astana q.

ИП DOC, 010000,  
Республика Казахстан, г.  
Астана

IP DOC, 010000,  
Kazakhstan, Astana



## МАЗМУНЫ – СОДЕРЖАНИЕ – CONTENT

### ӘЛЕУМЕТТІК-ЭКОНОМИКАЛЫҚ ЖӘНЕ ҚҰҚЫҚ ҒЫЛЫМДАРЫ – СОЦИАЛЬНО- ЭКОНОМИЧЕСКИЕ И ЮРИДИЧЕСКИЕ НАУКИ – SOCIO-ECONOMIC AND LEGAL SCIENCES

Zhyldyz Alzhanbaeva

**ANALYSIS AND CLASSIFICATION OF MAJOR CHALLENGES IN CREATING A BUSINESS-  
ENABLING ENVIRONMENT IN KYRGYZ REPUBLIC.....6**

Абраева Салтанат Диасовна

**ВЛИЯНИЕ ВОЛАТИЛЬНОСТИ МИРОВЫХ РЫНКОВ НА СТРАТЕГИЮ ХЕДЖИРОВАНИЯ  
ФИЗИЧЕСКИХ ПОЗИЦИЙ ЗЕРНОВЫХ И МАСЛИЧНЫХ КУЛЬТУР .....17**

Жұмасан Жамиля Сабырқызы

**ИСПОЛЬЗОВАНИЕ СМАРТ-КОНТРАКТОВ И ДЕЦЕНТРАЛИЗОВАННЫХ РЕЕСТРОВ ДЛЯ  
ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ПРОЕКТАМИ В УСЛОВИЯХ  
ЦИФРОВИЗАЦИИ.....21**

Kinetova Nuray Kuanyshkyzy, Ismailova Rymkul Amanzholovna

**GAME LEARNING IN PROJECT MANAGEMENT EDUCATION: PROBLEMS AND SOLUTIONS..... 33**

Петрова Алла Константиновна

**ПРОТИВОДЕЙСТВИЕ КОРРУПЦИИ: РОЛЬ ГРАЖДАНСКОГО ОБЩЕСТВА В  
МОНИТОРИНГЕ И КОНТРОЛЕ ЗА ДЕЯТЕЛЬНОСТЬЮ ГОСУДАРСТВЕННЫХ ОРГАНОВ В  
КАЗАХСТАНЕ .....43**

Yergazy Aitzhan Muslimuly

**METHODOLOGICAL MODEL FOR INTEGRATING AI TOOLS INTO BUSINESS PROCESSES  
BASED ON THE AGILE APPROACH .....46**

Темербаев Ержан Жуматаевич

**МОДЕЛИ ОТВЕТСТВЕННОСТИ ЗА АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ В  
ПРОИЗВОДСТВЕННЫХ ОРГАНИЗАЦИЯХ.....59**

Мустафин Куаныш

**СТАНДАРТИЗАЦИЯ И КОМПЛАЕНС В МУВИНГОВОЙ ИНДУСТРИИ США:  
ОПЕРАЦИОННАЯ МОДЕЛЬ МАСШТАБИРОВАНИЯ ЧЕРЕЗ ФРАНЧАЙЗИНГ .....66**

### ТЕХНИКАЛЫҚ ҒЫЛЫМДАР - ТЕХНИЧЕСКИЕ НАУКИ - TECHNICAL SCIENCE

Dauletbay Assiyat Bagdatkyzy, Shamil Nartay Muratuly, Serikov Mansur Kuanyshpayevich

**FROM CLASSROOM TO CAREER: LEVERAGING PEER-TO-PEER SKILL EXCHANGE TO  
REDUCE THE EMPLOYABILITY GAP.....73**

Нажим Танат Муратулы

**АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ ТОЧНОСТИ В ТЕХНОЛОГИИ FDM-печати.....78**

Khassanov Fakhreddin, Shaikhanova Aigul

**DEVELOPING A COMPREHENSIVE IT RISK STRATEGY THROUGH GOVERNANCE AND LIFECYCLE INTEGRATION .....84**

Syzdykhan Fatima, Baegizova Aigulim

**SYSTEMATIZATION OF CYBER THREATS AND A PROTECTION MODEL FOR UAV INFORMATION AND CONTROL CHANNELS BASED ON NIST CSF 2.0.....91**

Rysbek Beibarys

**ON-BOARD LIGHTWEIGHT ANOMALY DETECTION FOR UAV AUTOPILOT TELEMETRY USING TINYML AND SAFETY INCIDENT SCORING.....97**

Бисимбаева Аружан Танатовна

**СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ RANDOM FOREST И SUPPORT VECTOR MACHINE ДЛЯ КЛАССИФИКАЦИИ ЗЕМНОГО ПОКРОВА УРБАНИЗИРОВАННОЙ ТЕРРИТОРИИ Г. АСТАНА ПО ДАННЫМ SENTINEL-2 .....110**

Syzdykhan Fatima, Baegizova Aigulim

**MODELING AND QUANTITATIVE EVALUATION OF CYBER-RESILIENCE IN UAV CONTROL SYSTEMS UNDER MALICIOUS SOFTWARE INFLUENCE .....122**

Sadykhanov Aben

**FORECASTING TAX REVENUES TO THE BUDGET OF KAZAKHSTAN USING MACHINE LEARNING.....130**

Balmakhanov Danial Talgatuly, Aldashev Aslan Kanatovich, Osserbay Amandos Nurboluly

**DEVELOPMENT AND EVALUATION OF AN AI-BASED INTRUSION DETECTION SYSTEM FOR NETWORK TRAFFIC.....145**

Жигер Емжаев

**ВНЕДРЕНИЕ МОДУЛЬНОЙ СИСТЕМЫ ОБУЧЕНИЯ РАБОЧЕГО ПЕРСОНАЛА В УСЛОВИЯХ КРУПНОЙ ПРОМЫШЛЕННОЙ ОРГАНИЗАЦИИ: ФАКТОРЫ ЭФФЕКТИВНОСТИ И ОРГАНИЗАЦИОННЫЕ РИСКИ .....149**

Albina Mussakhan, Moldir Omar, Talgatova Ayaulym

**MACHINE LEARNING-BASED DETECTION OF SECURITY VULNERABILITIES IN SOURCE CODE.....155**

Қожа Адай Қозыұлы

**СОВЕРШЕНСТВОВАНИЕ МЕТОДОВ ДИАГНОСТИКИ ХОДОВОЙ ЧАСТИ ЭЛЕКТРОМОБИЛЕЙ НА СТАНЦИЯХ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ ГОРОДА АСТАНЫ .....160**

Salim Togzhan Turlybekkyzy, Kuatbayeva Akmaral Alikhanovna

**A COMPUTATIONAL MODEL FOR SMART CITY SUSTAINABILITY ASSESSMENT BASED ON INTEGRATED INDICATORS .....164**

Karayev Assadbek

**PATCHTST METHOD FOR FORECASTING ENERGY CONSUMPTION BASED ON HISTORICAL DATA AND WEATHER CONDITIONS.....176**

Бақытбекқызы Анар

**ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ ОБРАЗОВАТЕЛЬНЫХ ПЛАТФОРМ (MOODLE, BLACKBOARD, GOOGLE CLASSROOM) И РАЗРАБОТКА СТРАТЕГИИ ЗАЩИТЫ ДАННЫХ .....183**

Zhakhangir Temir, Symbat Nurgaliyeva

**A COMPARATIVE REVIEW OF THE ARCHITECTURE AND APPLICATION METHODS OF OPEN-SOURCE SIMULATORS FOR TEACHING ROBOTICS AND IOT .....188**

Kussaiyn Dinmukhamed, Zhumadillayeva Ainur

**AI FACE RECOGNITION IN CROWDED PLACES: CHALLENGES, DIFFICULTIES, AND COMPARATIVE ANALYSIS.....195**

Калиева Қарлығаш Бейсенбекқызы

**ПОВЫШЕНИЕ КОЭФФИЦИЕНТА МОЩНОСТИ СИСТЕМЫ ЭЛЕКТРОСНАБЖЕНИЯ ЗЕРНОВОГО ЭЛЕВАТОРА ТОО «БУЛАНДЫ-АСТЫК» С ПРИМЕНЕНИЕМ ЧАСТОТНЫХ ПРЕОБРАЗОВАТЕЛЕЙ .....204**

## **ПӘНДЕР АРАЛЫҚ ҒЫЛЫМДАР – МЕЖДИСЦИПЛИНАРНЫЕ НАУКИ – INTERDISCIPLINARY SCIENCES**

Gazez Aishat Aibatkyzy

**EMOTIONAL EXPRESSION IN TWO LANGUAGES: BILINGUAL PERSPECTIVES ON LANGUAGE CHOICE AND EMOTIONAL AUTHENTICITY .....213**

Mamataeva Ramina Adilgazyevna, Sakibayev Spartak Razakhovich

**ARTIFICIAL INTELLIGENCE IN EDUCATION.....218**

ӨЛЕУМЕТТИК-ЭКОНОМИКАЛЫҚ ЖӘНЕ ҚҰҚЫҚ ҒЫЛЫМДАРЫ –  
СОЦИАЛЬНО-ЭКОНОМИЧЕСКИЕ И ЮРИДИЧЕСКИЕ НАУКИ – SOCIO-  
ECONOMIC AND LEGAL SCIENCES

**Zhyldyz Alzhanbaeva**

Business Development Expert  
(Bishkek, Kyrgyzstan)

**ANALYSIS AND CLASSIFICATION OF MAJOR CHALLENGES IN CREATING A  
BUSINESS-ENABLING ENVIRONMENT IN KYRGYZ REPUBLIC**

**Abstract:** This article examines the major challenges to creating a business-enabling environment in the Kyrgyz Republic through an integrated analytical, empirical, and legal approach. The study proceeds from the premise that the effectiveness of a business environment depends not only on the existence of formal legal and regulatory frameworks, but on the quality of their implementation, coherence, and institutional enforcement. Drawing on business perception surveys, international institutional assessments, national analytical reports, and legal analysis, the article identifies and classifies the core constraints affecting business activity in Kyrgyzstan.

The findings demonstrate that regulatory complexity and instability, inconsistent law enforcement, governance-related risks, limited access to finance, and infrastructure deficiencies constitute a mutually reinforcing system of barriers. The research confirms that the principal challenge lies in the gap between formally established legal norms and their practical application. Frequent regulatory changes, overlapping legal regimes, and broad administrative discretion undermine legal certainty and increase transaction costs, particularly for small and medium-sized enterprises.

From a legal and institutional perspective, the business-enabling environment is conceptualized as a legally constructed system whose effectiveness depends on regulatory coherence, predictability, and enforceability. The article concludes that fragmented and isolated reform measures are insufficient to address systemic constraints and emphasizes the importance of an integrated approach combining regulatory quality, consistent law enforcement, effective legal protection mechanisms, and institutional capacity. The study contributes to the academic literature on business environment reform in transition economies and provides a structured analytical basis for further legal and policy-oriented research.

**Keywords:** Business-enabling environment; regulatory quality; legal certainty; law enforcement; governance; access to finance; infrastructure constraints; transition economy; Kyrgyz Republic.

**Introduction.** The creation of a business-enabling environment is widely recognized as a fundamental prerequisite for sustainable economic growth, private sector development, and investment attraction. In transition economies, this task is particularly complex, as institutional transformation, legal reforms, and market liberalization often evolve unevenly and are accompanied by structural inefficiencies. The quality of the business environment directly affects entrepreneurial activity, competitiveness, and the long-term resilience of national economies.

The Kyrgyz Republic represents a typical case of a small open economy undergoing prolonged transition. Since gaining independence, the country has implemented a series of economic and legal reforms aimed at promoting private initiative, reducing state involvement in economic activities, and integrating into regional and global markets. These reforms have included the adoption of business-related legislation, tax system restructuring, investment promotion measures, and initiatives to simplify administrative procedures. However, despite these efforts, the overall business environment remains constrained by persistent systemic challenges.

Empirical observations and analytical assessments consistently indicate a gap between formal regulatory frameworks and their practical implementation. While the legal architecture governing entrepreneurship appears relatively comprehensive, businesses continue to face regulatory uncertainty, inconsistent enforcement of rules, and elevated compliance costs. These issues are further exacerbated by governance weaknesses, limited institutional capacity, and deficiencies in infrastructure and financial systems.

In this context, improving the business-enabling environment in Kyrgyzstan is not merely a technical or regulatory issue but a broader institutional challenge. Addressing it requires a nuanced understanding of how legal, administrative, financial, and structural factors interact to shape business behavior. A fragmented or poorly functioning business ecosystem not only discourages domestic entrepreneurship but also undermines foreign investment and economic diversification efforts.

The purpose of this article is to analyze and classify the major challenges hindering the creation of a business-enabling environment in Kyrgyzstan. By adopting an analytical and systematic approach, the study seeks to move beyond descriptive assessments and provide a structured understanding of the core obstacles affecting business development. This approach allows for the identification of interrelated problem areas and creates a foundation for evidence-based policy recommendations.

Despite ongoing reform efforts, the business environment in Kyrgyzstan continues to face deep-rooted and multidimensional challenges that limit its effectiveness and predictability. The central problem lies not only in the existence of regulatory and institutional barriers, but in their systemic nature and cumulative impact on entrepreneurial activity. These barriers affect businesses at all stages of their lifecycle, from market entry and operation to expansion and exit.

One of the most prominent issues is regulatory inefficiency. Although legislation governing business activities aims to streamline procedures and enhance transparency, entrepreneurs frequently encounter excessive administrative requirements, overlapping competencies among state authorities, and unclear procedural guidelines. The lack of regulatory coherence leads to delays, discretionary decision-making, and increased transaction costs. As a result, compliance with formal rules often becomes burdensome, particularly for small and medium-sized enterprises (SMEs), which typically lack sufficient legal and administrative resources.

Closely linked to regulatory inefficiency is the problem of inconsistent enforcement. Differences in interpretation and application of laws across regions and institutions generate legal uncertainty and undermine the principle of equal treatment. Businesses are often exposed to unpredictable inspections, conflicting requirements, and ad hoc administrative practices. This environment weakens trust in public institutions and reduces incentives for formalization and long-term investment.

Governance-related challenges further compound these problems. Corruption risks, limited accountability mechanisms, and weak institutional oversight continue to distort business–state interactions. Informal practices, such as unofficial payments or negotiated compliance, not only increase operational costs but also distort competition by placing compliant firms at a disadvantage. For many entrepreneurs, especially in highly regulated sectors, governance failures represent one of the most significant obstacles to sustainable business operations.

Financial constraints constitute another critical dimension of the problem. Access to affordable finance remains limited due to high interest rates, stringent collateral requirements, and underdeveloped financial instruments. SMEs and start-ups are particularly affected, as they often lack the assets or credit history required to obtain bank financing. In parallel, insufficient financial literacy and weak support mechanisms further restrict the ability of businesses to mobilize capital for growth and innovation.

Infrastructure and digitalization gaps add an additional layer of complexity. Inadequate transport networks, unreliable energy supply, and uneven access to digital services increase operational risks and limit market access, especially for businesses located outside major urban centers. While digital solutions have the potential to reduce administrative burdens and enhance transparency, their implementation remains fragmented and uneven.

Taken together, these challenges form a mutually reinforcing system of constraints that inhibit the development of a truly business-enabling environment in Kyrgyzstan. The absence of a comprehensive analytical classification of these challenges limits the effectiveness of reform efforts, as policy interventions often address isolated symptoms rather than underlying structural causes. This article addresses this gap by systematically identifying and classifying the major obstacles to business development, thereby providing a conceptual framework for more coherent and targeted reforms.

### **Analytical Framework and Classification of Challenges**

To provide a structured and policy-relevant assessment of the business-enabling environment in the Kyrgyz Republic, this study applies an integrated analytical framework that classifies existing challenges into interrelated categories reflecting the core dimensions of business activity. Rather than examining individual constraints in isolation, the framework emphasizes their cumulative and mutually reinforcing nature. The classification is informed by institutional analysis, regulatory review, and empirical evidence derived from business perception surveys conducted by the International Business Council (IBC), as well as official data from national authorities.

The first major category of constraints relates to regulatory and legal barriers. Although Kyrgyzstan has established a relatively comprehensive legal framework governing entrepreneurial activity, the effectiveness of this framework is undermined by regulatory complexity and implementation gaps.<sup>1</sup> Businesses frequently report excessive administrative requirements, overlapping mandates among public authorities, and insufficient procedural clarity. These issues are particularly evident in licensing, inspections, and compliance-related processes. According to business surveys, regulatory uncertainty and administrative burden consistently rank among the most significant impediments to business operations. A large proportion of respondents identify licensing procedures and unpredictable inspections as sources of increased costs and delays, especially for small and medium-sized enterprises.

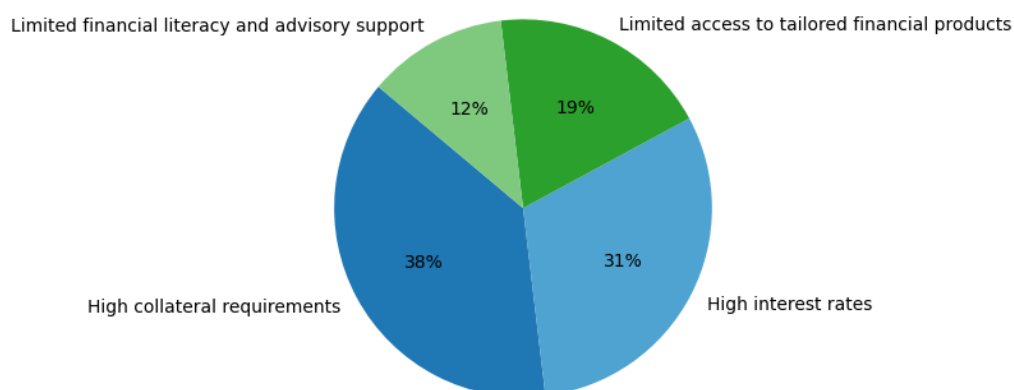
---

<sup>1</sup>Ministry of Economy and Commerce of the Kyrgyz Republic Entrepreneurship Development Reports; International Business Council, Investment Climate and Business Surveys, 2019–2023

This regulatory burden is compounded by inconsistent law enforcement, which constitutes a second, closely related category of challenges. Variations in the interpretation and application of legal norms across institutions and regions generate legal uncertainty and weaken the predictability of the business environment. Entrepreneurs often face divergent requirements from different regulatory bodies, even when operating under the same legal provisions. Such inconsistencies erode trust in public institutions and reduce incentives for long-term investment. Empirical data suggest that businesses perceive enforcement-related risks as comparable in severity to formal regulatory barriers, highlighting the importance of implementation quality rather than legislative design alone.<sup>2</sup>

Governance-related constraints represent a third critical dimension shaping the business climate. Weak institutional capacity, limited accountability mechanisms, and persistent corruption risks continue to affect interactions between businesses and the state. Informal practices, including unofficial payments and discretionary decision-making, distort market competition and disproportionately affect smaller firms with limited bargaining power. Business perception surveys indicate that corruption-related risks remain a central concern, particularly in areas involving frequent administrative contact, such as inspections, taxation, and customs procedures. These governance challenges not only increase transaction costs but also undermine the credibility of reform initiatives aimed at improving the business environment.<sup>3</sup>

Figure 1. Distribution of Key Financial Constraints Reported by Businesses



Financial constraints form another major category within the analytical framework. Access to finance remains limited due to high interest rates, strict collateral requirements, and the underdevelopment of alternative financing instruments. Survey data demonstrate that micro and small enterprises experience significantly greater difficulties in obtaining external financing compared to medium-sized firms. As illustrated in **Figure 1**, which presents a circular distribution of reported financing barriers, the most frequently cited obstacles include collateral requirements, high borrowing costs, and limited availability of tailored financial products. The predominance of internal funds and informal financing sources further underscores structural weaknesses in the financial system and constrains firms' capacity for expansion, innovation, and productivity enhancement.

In addition to regulatory, institutional, and financial barriers, infrastructure-related constraints play a significant role in shaping business performance. Inadequate transport

<sup>2</sup> Ministry of Justice of the Kyrgyz Republic, Analysis of Law Enforcement Practice (2024)

<sup>3</sup> International Business Council, Anti-Corruption and Governance Survey Findings

networks, unreliable energy supply, and uneven digital connectivity increase operational risks and limit market access, particularly for firms located outside major urban centers. These constraints are especially pronounced for export-oriented and logistics-intensive sectors, where efficiency and reliability are critical. Business surveys reveal notable regional disparities in infrastructure quality, which translate into uneven competitive conditions across the country.

Figure 2. Composition of Infrastructure-Related Barriers to Business Operations

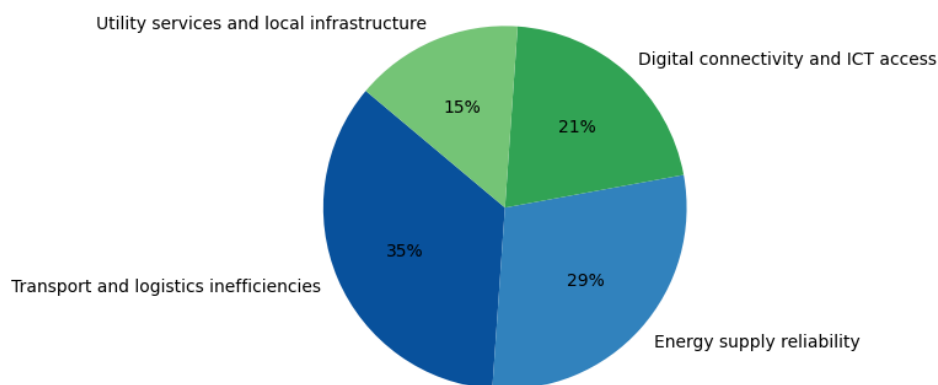


**Figure 2**, a circular diagram summarizing infrastructure-related obstacles reported by firms, highlights transport and energy reliability as the most pressing concerns, followed by digital connectivity.

Importantly, the challenges identified in this framework do not operate independently. Regulatory complexity often interacts with governance weaknesses, amplifying opportunities for discretionary enforcement and informal practices. Financial constraints are exacerbated by infrastructure deficiencies that reduce profitability and increase operational risks, thereby affecting firms' creditworthiness. Similarly, weak institutional capacity limits the effectiveness of reforms aimed at simplifying regulations or improving access to finance. The interaction of these factors creates a reinforcing cycle of constraints that collectively undermine the business-enabling environment.

By classifying challenges into these interconnected domains, the analytical framework provides a coherent basis for understanding the structural nature of business environment constraints in Kyrgyzstan. This approach allows for a more nuanced interpretation of empirical evidence and highlights the limitations of fragmented or sector-specific reform measures. Instead, it underscores the need for coordinated policy interventions that simultaneously address regulatory quality, institutional performance, financial accessibility, and infrastructure development. The following sections build on this framework to examine empirical findings in greater depth and to derive policy-relevant implications for improving the business environment.

### **Empirical Findings and Discussion**

This section presents an empirical analysis of the business-enabling environment in the Kyrgyz Republic based on a combination of national and international data sources. The analysis triangulates findings from business perception surveys, international institutional assessments, and official analytical reports published by national authorities. The use of multiple sources allows for cross-validation of findings and reduces the limitations associated with reliance on a single dataset.

Empirical evidence consistently demonstrates that regulatory and administrative barriers remain among the most significant constraints on business activity in Kyrgyzstan. According to the surveys, businesses repeatedly identify regulatory uncertainty, excessive administrative procedures, and inspection-related risks as primary obstacles to operations.<sup>4</sup> These findings are supported by international firm-level data from the which indicate that a substantial share of firms' senior management time is devoted to dealing with regulatory compliance and interactions with public authorities.<sup>5</sup> This diversion of managerial resources negatively affects productivity and firm performance.

Inconsistent law enforcement emerges as a structurally significant issue across empirical sources. While Kyrgyzstan has undertaken legislative reforms aimed at standardizing business regulation, variations in interpretation and application of legal norms persist across institutions and regions. This problem is documented in the Ministry of Justice of the Kyrgyz Republic Reports which highlights discrepancies in enforcement practices and insufficient methodological guidance for regulatory bodies.<sup>6</sup> Business perceptions confirm that enforcement-related risks are perceived as comparable in severity to formal regulatory barriers, underscoring that implementation quality plays a decisive role in shaping the business climate.

Governance-related challenges are another empirically substantiated constraint. According to Transparency International, Corruption Perceptions Index 2022<sup>7</sup>, the Kyrgyz Republic continues to face systemic governance weaknesses, particularly in public administration and regulatory enforcement. Business-level evidence from the International Business Council Anti-Corruption and Governance Survey 2021 indicates that informal practices remain a concern in areas involving frequent administrative contact, including inspections, tax administration, and customs procedures. These governance failures increase transaction costs and distort competitive conditions, disproportionately affecting small and medium-sized enterprises with limited capacity to absorb compliance risks.

Infrastructure-related constraints further compound the challenges identified above. According to the Ministry of Economy and Commerce of the Kyrgyz Republic, Infrastructure and Regional Development Reports, businesses operating outside major urban centers face higher logistics costs, unreliable energy supply, and uneven access to digital infrastructure.<sup>8</sup> These findings are corroborated by business perception, highlights transport and energy reliability as the most significant infrastructure-related obstacles, particularly for export-oriented and logistics-intensive firms. Although digital connectivity has improved in recent years, the Ministry of Economy and Commerce of the Kyrgyz Republic, Digital Economy Development Report 2023 notes persistent regional disparities that limit the effectiveness of e-government services and digital compliance mechanisms.<sup>9</sup>

A key empirical insight emerging from this multi-source analysis is the interconnected nature of business environment constraints. Regulatory complexity increases opportunities for discretionary enforcement, thereby amplifying governance-related risks. Financial constraints are exacerbated by infrastructure deficiencies that reduce firm profitability and creditworthiness.

---

<sup>4</sup> International Business Council Business Environment Survey 2019, International Business Council Business Environment Survey 2021, and International Business Council Investment Climate Survey 2023

<sup>5</sup> World Bank Enterprise Surveys: Kyrgyz Republic 2023

<sup>6</sup> Ministry of Justice of the Kyrgyz Republic, Review of Law Enforcement Practice in the Sphere of Entrepreneurial Activity, 2022

<sup>7</sup> Transparency International, Corruption Perceptions Index 2022

<sup>8</sup> Ministry of Economy and Commerce of the Kyrgyz Republic, Infrastructure and Regional Development Report, 2022

<sup>9</sup> Ministry of Economy and Commerce of the Kyrgyz Republic, Digital Economy Development Report, 2023

Weak institutional capacity undermines the effectiveness of reforms aimed at simplifying regulations or expanding access to finance. These interdependencies create a self-reinforcing cycle of constraints that limits the overall impact of isolated policy interventions.

Overall, empirical evidence from national and international sources confirms that challenges to the business-enabling environment in the Kyrgyz Republic are systemic rather than episodic. While individual reforms have addressed specific issues, their effectiveness has been constrained by insufficient coordination, uneven implementation, and institutional weaknesses. These findings underscore the need for integrated and sequenced policy responses that simultaneously address regulatory quality, governance capacity, financial accessibility, and infrastructure development. The following section translates these empirical insights into concrete policy implications and recommendations.

### **Legal Assessment of the Business-Enabling Environment in the Kyrgyz Republic**

From a legal standpoint, the business-enabling environment in the Kyrgyz Republic is shaped by a complex system of normative legal acts regulating entrepreneurial activity, investment, taxation, competition, administrative procedures, and dispute resolution. The existing legal framework is primarily based on the Constitution of the Kyrgyz Republic, the Civil Code of the Kyrgyz Republic, the Tax Code of the Kyrgyz Republic, and a wide range of framework and sector-specific laws governing economic activity. Formally, this system reflects the core principles of a market economy, including freedom of entrepreneurship, equality of economic actors, protection of property rights, and non-interference of the state in lawful business activities. However, the practical effectiveness of these principles remains constrained by structural legal and institutional deficiencies.

A central legal issue affecting the business environment is the fragmentation and instability of business-related legislation. Entrepreneurial activity in Kyrgyzstan is regulated by numerous laws, including legislation on licensing and permits, investment activity, inspections of business entities, public procurement, and competition. While each of these legal instruments pursues legitimate regulatory objectives, their cumulative effect often results in regulatory overlap and normative inconsistency. Frequent amendments to the Tax Code, licensing legislation, and administrative procedures complicate legal compliance and reduce predictability for businesses. From the perspective of legal certainty, such instability undermines the ability of entrepreneurs to plan economic activity and assess legal risks over the medium and long term.

The Law of the Kyrgyz Republic on Licensing and Permit System, together with subordinate regulatory acts, establishes the legal basis for access to regulated economic activities. In practice, however, the coexistence of general licensing rules with sector-specific requirements creates legal ambiguity. Businesses often encounter situations where compliance with one regulatory regime does not fully satisfy the requirements of another, leading to repeated administrative interactions and increased transaction costs. This problem reflects broader challenges in regulatory coordination and legislative coherence.

Inconsistent law enforcement represents another fundamental legal constraint. Despite the existence of unified legal norms, their interpretation and application vary across administrative bodies and territorial units. This issue is particularly evident in the implementation of legislation governing inspections of business entities, tax administration, and customs regulation. The Law of the Kyrgyz Republic on the Procedure for Conducting Inspections of Business Entities formally aims to limit excessive administrative interference. Nevertheless, broad discretionary powers granted to supervisory authorities allow for divergent enforcement practices. From a legal

perspective, such discretion, when insufficiently constrained by procedural safeguards, increases the risk of arbitrary decision-making and weakens the principle of equality before the law.

Administrative procedures play a central role in shaping the legal experience of businesses. The regulatory system relies extensively on permits, approvals, registrations, and inspections, which place entrepreneurs in continuous interaction with public authorities. Although administrative procedures are intended to protect public interests, their excessive complexity often transforms them into sources of legal risk. The Law of the Kyrgyz Republic on Administrative Procedures establishes general principles governing administrative decision-making, including legality, proportionality, and transparency. However, the practical implementation of these principles remains uneven, particularly at the local level, where institutional capacity and legal expertise vary significantly.

Legal protection mechanisms available to businesses constitute another critical dimension of the business-enabling environment. The judicial system, including courts of general jurisdiction and economic courts, formally provides avenues for challenging administrative acts and resolving commercial disputes. In addition, alternative dispute resolution mechanisms, such as arbitration, are recognized under national legislation. Despite the availability of these mechanisms, businesses often perceive legal remedies as slow, unpredictable, or costly. Difficulties related to enforcement of judicial decisions further weaken confidence in formal dispute resolution and reduce the deterrent effect of legal accountability for administrative bodies.

Financial relations between businesses and the state also reveal important legal implications. Access to finance is influenced not only by market conditions but by the legal framework governing secured transactions, collateral registration, and insolvency. The Civil Code of the Kyrgyz Republic and legislation on pledge and bankruptcy establish the legal basis for creditor and debtor relations. In practice, however, delays and uncertainties in collateral enforcement and insolvency proceedings increase legal risks for financial institutions. As a result, lenders adopt conservative risk management strategies, transferring legal uncertainty to borrowers through high interest rates and stringent collateral requirements. This legal dimension significantly affects the availability of credit, particularly for small and medium-sized enterprises.

Infrastructure development and public–private economic interaction further illustrate the legal nature of business environment challenges. Legal frameworks governing public procurement, concession agreements, and public–private partnerships define the conditions under which private businesses may participate in infrastructure projects. While relevant legislation establishes formal procedures and guarantees, uncertainty regarding contractual enforcement, regulatory stability, and dispute resolution discourages long-term private investment. From a legal perspective, the predictability and enforceability of contractual obligations are essential for fostering sustainable cooperation between the public and private sectors.

Investment activity in the Kyrgyz Republic is regulated by legislation on investments, which formally guarantees protection of investors' rights, non-discrimination, and access to dispute resolution mechanisms. Nevertheless, empirical evidence suggests that investors remain concerned about regulatory changes, enforcement practices, and institutional stability. These concerns highlight the gap between formal legal guarantees and their practical realization, reinforcing the importance of consistent application of investment-related norms.

Taken together, the analysis demonstrates that challenges in the business-enabling environment of the Kyrgyz Republic stem not from the absence of legal regulation, but from qualitative deficiencies in its structure and implementation. The legal system provides extensive

normative coverage of business activity; however, fragmentation, instability, broad administrative discretion, and limited effectiveness of legal protection mechanisms undermine its practical value for entrepreneurs.

In conclusion, the business-enabling environment in the Kyrgyz Republic should be understood as a legally constructed system in which the quality of legislation, administrative practice, and institutional capacity are closely interconnected. Sustainable improvement of this environment depends on strengthening legal certainty, ensuring consistent and predictable law enforcement, and enhancing the effectiveness of judicial and administrative safeguards for economic actors. From a legal perspective, the development of a favorable business environment is inseparable from the broader task of consolidating the rule of law and ensuring credible protection of economic rights within the national legal system.

**Conclusion.** This study has examined the major challenges to creating a business-enabling environment in the Kyrgyz Republic through an integrated analytical, empirical, and legal perspective. The analysis demonstrates that, despite the existence of a formally developed legal and regulatory framework governing entrepreneurial activity, the practical functioning of the business environment remains constrained by systemic and interrelated challenges. These challenges are neither episodic nor sector-specific; rather, they reflect deeper structural deficiencies in regulatory design, law enforcement practices, institutional capacity, and the overall level of legal certainty.

The findings indicate that regulatory complexity and instability, inconsistent enforcement of legal norms, governance-related risks, limited access to finance, and infrastructure deficiencies jointly shape the business climate. Importantly, the study confirms that the core problem does not lie in the absence of legislation as such, but in the qualitative gap between formal legal norms and their practical implementation. Frequent regulatory changes, overlapping legal regimes, and broad administrative discretion undermine predictability and increase legal and transaction costs for businesses, with particularly adverse effects on small and medium-sized enterprises.

Empirical evidence drawn from national and international sources further reveals that these constraints tend to reinforce one another. Regulatory ambiguity amplifies governance risks; weak legal protection mechanisms reduce trust in formal institutions; financial constraints are exacerbated by legal uncertainty surrounding collateral enforcement and insolvency procedures; and infrastructure gaps intensify regional disparities in business conditions. As a result, reform efforts that target individual aspects of the business environment in isolation have produced limited and often short-lived outcomes, underscoring the need for a more coherent and systemic approach.

From a legal and institutional perspective, the business-enabling environment in the Kyrgyz Republic should therefore be understood as a legally constructed system whose effectiveness depends on the coherence, stability, and enforceability of its underlying rules. Sustainable improvement requires not only regulatory simplification, but also a consistent application of the rule of law, greater uniformity in law enforcement, and enhanced credibility of legal safeguards available to economic actors.

Building on the conclusions of this study, a set of interrelated policy recommendations can be proposed to address the structural nature of the identified challenges and to strengthen the overall business-enabling environment in the Kyrgyz Republic.

First, regulatory coherence and legal certainty should be enhanced. Business-related legislation requires further systematization in order to reduce fragmentation and overlaps

between general and sector-specific norms. Regulatory reforms should place greater emphasis on stability and predictability, limiting frequent amendments and ensuring adequate transition periods that allow businesses to adapt to new legal requirements. Strengthening regulatory impact assessment mechanisms would contribute to more informed legislative decision-making and reduce unintended negative effects on entrepreneurial activity.

Second, greater consistency and transparency in law enforcement should be ensured. The development and application of unified methodological guidelines for the implementation of business-related legislation across institutions and regions would reduce discrepancies in enforcement practices. Limiting excessive administrative discretion through clearer procedural rules and standardized approaches would enhance legal predictability and reinforce the principle of equality before the law.

Third, administrative justice and legal protection mechanisms should be strengthened. Effective access to remedies against unlawful or disproportionate administrative actions is essential for safeguarding business rights. Improving the efficiency, predictability, and enforceability of judicial and administrative review mechanisms would increase trust in formal legal institutions and reduce incentives for reliance on informal practices.

Fourth, legal barriers affecting access to finance should be addressed. The legal frameworks governing secured transactions, collateral registration, and insolvency procedures should operate in a manner that reduces legal risk for both lenders and borrowers. Enhancing the effectiveness and predictability of these mechanisms would contribute to lower financing costs and broader access to credit, particularly for small and medium-sized enterprises.

Fifth, the legal framework governing public–private economic interaction should be reinforced. Clear, predictable, and enforceable legal rules related to public procurement, concessions, and public–private partnerships are critical for attracting private investment, especially in infrastructure development. Strengthening contractual enforcement and dispute resolution mechanisms would improve investor confidence and support long-term private sector engagement.

Finally, reforms aimed at improving the business environment should be implemented through an integrated and coordinated approach. Given the interconnected nature of regulatory, institutional, financial, and infrastructural constraints, fragmented policy measures are unlikely to produce sustainable results without parallel improvements in legal enforcement and institutional capacity.

In sum, improving the business-enabling environment in the Kyrgyz Republic constitutes both an economic and a legal challenge. The effectiveness of future reforms will depend on their ability to strengthen legal certainty, institutional credibility, and the practical enforceability of business-related norms. By adopting a systemic and legally grounded approach, the Kyrgyz Republic can create more predictable and transparent conditions for entrepreneurship and investment, thereby supporting long-term economic development and greater resilience of the national economy.

### References:

1. Asian Development Bank. (2020). Financial sector assessment: Kyrgyz Republic. Manila: Asian Development Bank.
2. Constitution of the Kyrgyz Republic. (2010, as amended)
3. Civil Code of the Kyrgyz Republic. (1996, as amended)

4. International Business Council. (2019). Business environment survey. Bishkek: International Business Council.
5. International Business Council. (2021). Business environment and investment climate survey. Bishkek: International Business Council.
6. International Business Council. (2021). Anti-corruption and governance survey. Bishkek: International Business Council.
7. International Business Council. (2021). SME finance survey. Bishkek: International Business Council.
8. International Business Council. (2023). Investment climate survey. Bishkek: International Business Council.
9. Law of the Kyrgyz Republic on Administrative Procedures. (2015, as amended)
10. Law of the Kyrgyz Republic on Bankruptcy (Insolvency). (1997, as amended)
11. Law of the Kyrgyz Republic on Investments in the Kyrgyz Republic. (2003, as amended)
12. Law of the Kyrgyz Republic on Licensing and Permit System. (2013, as amended)
13. Law of the Kyrgyz Republic on Public Procurement. (2015, as amended)
14. Law of the Kyrgyz Republic on Public–Private Partnership. (2019, as amended)
15. Law of the Kyrgyz Republic on the Procedure for Conducting Inspections of Business Entities. (2007, as amended)
16. Ministry of Economy and Commerce of the Kyrgyz Republic. (2022). Infrastructure and regional development report
17. Ministry of Economy and Commerce of the Kyrgyz Republic. (2023). Digital economy development report
18. Ministry of Justice of the Kyrgyz Republic. (2021). Review of law enforcement practice in the sphere of entrepreneurial activity
19. Tax Code of the Kyrgyz Republic. (2022)
20. Transparency International. (2022). Corruption perceptions index 2022. Berlin: Transparency International.
21. World Bank. (2023). Enterprise surveys: Kyrgyz Republic. Washington, DC: World Bank.

УДК 339.13:338.43

Абраева Салтанат Диасовна

Независимый исследователь  
(г. Астана, Казахстан)

## ВЛИЯНИЕ ВОЛАТИЛЬНОСТИ МИРОВЫХ РЫНКОВ НА СТРАТЕГИЮ ХЕДЖИРОВАНИЯ ФИЗИЧЕСКИХ ПОЗИЦИЙ ЗЕРНОВЫХ И МАСЛИЧНЫХ КУЛЬТУР

**Аннотация:** В современных условиях мировой торговли зерновыми и масличными культурами участники рынков сталкиваются с высокой степенью ценовой волатильности, что создает существенные риски для производителей, торговых компаний, экспортеров и переработчиков. Волатильность цен на зерновые и масличные товары определяется множеством факторов, включая климатические изменения, макроэкономическую нестабильность, геополитические риски, спекулятивную активность на товарных биржах и структурные изменения в глобальной логистике. Цель данной статьи заключается в комплексном анализе влияния волатильности мировых рынков на стратегии хеджирования физических позиций зерновых и масличных культур. В статье рассматриваются теоретические аспекты управления ценовыми рисками, эмпирические результаты, основанные на оценке динамики волатильности ключевых товарных цен и эффективности различных стратегий хеджирования, а также обсуждаются практические последствия для участников аграрных рынков. Для достижения поставленной цели проведено эмпирическое исследование, включающее анализ исторической волатильности цен на фьючерсные контракты по пшенице, кукурузе и соевых бобах на крупнейших товарных биржах, а также оценка эффективности традиционных и адаптивных стратегий хеджирования. Основные результаты показывают, что высокая волатильность снижает эффективность статических стратегий хеджирования, требуя перехода к динамическим и гибридным подходам. Практическая значимость исследования заключается в формулировании рекомендаций для аграрных предприятий и трейдеров по оптимизации стратегии управления ценовыми рисками в условиях нестабильных рынков. Ключевые выводы подтверждают необходимость интеграции прогнозных моделей волатильности и риск-менеджмента в стратегическое планирование аграрных компаний. Методологическая основа исследования включает применение моделей оценки исторической и подразумеваемой волатильности, статистических методов измерения хедж-эффективности и анализа риск-параметров. Полученные результаты являются актуальными для научного сообщества, практиков аграрного бизнеса и финансовых аналитиков, занимающихся управлением рисками. Статья может служить основой для дальнейших исследований в области управления рисками на рынках сельскохозяйственных товаров.

**Ключевые слова:** волатильность рынка, хеджирование, зерновые культуры, масличные культуры, фьючерсы, риск-менеджмент, продуктивность торговли, финансовые деривативы, моделирование риска

**Введение.** Глобальные рынки зерновых и масличных культур играют ключевую роль в обеспечении продовольственной безопасности, формировании экспортных доходов и поддержании макроэкономической стабильности многих стран. В то же время данные рынки характеризуются высокой чувствительностью к внешним шокам, что проявляется в значительных колебаниях цен на сельскохозяйственные товары. Волатильность цен на пшеницу, кукурузу, сою и другие культуры существенно возросла в начале XXI века, что связано с усилением климатических рисков, ростом взаимосвязи товарных и финансовых рынков, а также увеличением объемов спекулятивного капитала на товарных биржах. Для участников аграрных рынков, оперирующих физическими позициями, данные процессы создают значительные риски, способные привести к снижению рентабельности, росту финансовых потерь и ухудшению инвестиционной привлекательности отрасли.

В условиях высокой ценовой неопределенности хеджирование становится одним из ключевых инструментов управления рисками. Использование производных финансовых инструментов, прежде всего фьючерсных и опционных контрактов, позволяет участникам рынка частично или полностью компенсировать негативные последствия неблагоприятных ценовых движений. Однако эффективность хеджирования напрямую зависит от уровня и структуры волатильности рынка. Традиционные статические стратегии хеджирования, предполагающие фиксированное соотношение между физической и срочной позицией, могут демонстрировать ограниченную эффективность в периоды резких и непредсказуемых ценовых колебаний. Это обуславливает необходимость глубокого анализа взаимосвязи между динамикой волатильности и результатами применения различных стратегий хеджирования.

Научный интерес к проблеме волатильности и хеджирования аграрных рынков отражен в работах ряда исследователей, анализирующих как теоретические аспекты ценообразования и управления рисками, так и эмпирические закономерности поведения цен на сельскохозяйственные товары. Вместе с тем, несмотря на значительное количество исследований, вопрос адаптации стратегий хеджирования физических позиций к условиям высокой волатильности остается недостаточно изученным, особенно в контексте современных глобальных шоков и структурных изменений мировой экономики. Цель данной статьи заключается в выявлении и анализе влияния волатильности мировых рынков на стратегию хеджирования физических позиций зерновых и масличных культур с использованием современных методов экономического анализа.

**Материалы и методы.** Эмпирическая часть исследования основана на анализе временных рядов цен на зерновые и масличные культуры, представленных фьючерсными контрактами, торгуемыми на ведущих мировых товарных биржах. В качестве объектов исследования выбраны фьючерсы на пшеницу, кукурузу и соевые бобы, поскольку данные культуры обладают высокой ликвидностью и репрезентативностью для мирового аграрного рынка. Источниками данных послужили официальные биржевые котировки CME Group и Euronext за период с 2005 по 2024 годы, что позволяет охватить различные фазы рыночного цикла, включая периоды высокой волатильности, обусловленные финансовыми кризисами и геополитическими событиями.

Для оценки волатильности использовались показатели исторической волатильности, рассчитанные на основе стандартного отклонения логарифмических доходностей, а также элементы подразумеваемой волатильности, извлеченные из цен опционных контрактов. Историческая волатильность позволяет оценить фактическую изменчивость цен в

прошлом, в то время как подразумеваемая волатильность отражает ожидания участников рынка относительно будущих ценовых колебаний. Для анализа эффективности хеджирования применялся метод минимизации дисперсии, основанный на оценке оптимального хедж-коэффициента с использованием регрессионного анализа. Эффективность хеджирования оценивалась путем сравнения дисперсии доходности незащищенной физической позиции и позиции, защищенной с использованием фьючерсных контрактов.

В рамках исследования также применялись динамические подходы к хеджированию, предполагающие регулярную корректировку хедж-коэффициента в зависимости от текущего уровня волатильности. Для этого использовались модели скользящего окна и элементы условной волатильности, позволяющие учитывать изменение рыночных условий во времени. Сравнительный анализ статических и динамических стратегий хеджирования позволил выявить различия в их эффективности в условиях низкой и высокой волатильности.

**Результаты.** Результаты эмпирического анализа показали, что волатильность цен на зерновые и масличные культуры имеет ярко выраженный циклический характер и существенно возрастает в периоды глобальных экономических и политических потрясений. В частности, значительные всплески волатильности были зафиксированы в период мирового финансового кризиса 2008–2009 годов, в период пандемии COVID-19, а также в условиях усиления геополитической напряженности на мировых товарных рынках. Анализ исторической волатильности продемонстрировал, что среднегодовые значения волатильности для фьючерсов на пшеницу и кукурузу в отдельные периоды превышали долгосрочные средние показатели более чем в два раза.

Оценка эффективности хеджирования показала, что статические стратегии хеджирования обеспечивают значительное снижение дисперсии доходности физической позиции в условиях умеренной волатильности. Однако в периоды резких ценовых колебаний их эффективность заметно снижается. В то же время динамические стратегии хеджирования, предполагающие адаптацию хедж-коэффициента к текущему уровню волатильности, демонстрируют более высокую устойчивость и обеспечивают дополнительное снижение ценового риска. Результаты регрессионного анализа подтвердили наличие статистически значимой зависимости между уровнем волатильности и оптимальным хедж-коэффициентом, что указывает на необходимость гибкого подхода к управлению хедж-позициями.

**Обсуждение.** Полученные результаты согласуются с выводами предыдущих исследований, подчеркивающих важность учета волатильности при разработке стратегий хеджирования на товарных рынках. Рост волатильности увеличивает неопределенность будущих ценовых движений и снижает предсказуемость результатов применения стандартных инструментов управления рисками. В этих условиях статические стратегии хеджирования, широко используемые в аграрном секторе, оказываются недостаточно эффективными. Динамические и комбинированные стратегии, напротив, позволяют более адекватно реагировать на изменения рыночной конъюнктуры и обеспечивать более высокий уровень защиты физических позиций.

В практическом плане результаты исследования свидетельствуют о необходимости интеграции моделей оценки и прогнозирования волатильности в систему риск-менеджмента аграрных компаний. Использование как исторической, так и

подразумеваемой волатильности позволяет учитывать не только прошлую динамику цен, но и ожидания участников рынка, что повышает качество принимаемых управленческих решений. Вместе с тем следует учитывать, что динамические стратегии хеджирования требуют более высокого уровня аналитической подготовки и сопровождаются дополнительными транзакционными издержками.

**Заключение.** В ходе исследования было установлено, что волатильность мировых рынков оказывает существенное влияние на стратегию хеджирования физических позиций зерновых и масличных культур. Рост ценовой неопределенности снижает эффективность традиционных статических подходов к хеджированию и требует перехода к более гибким и адаптивным стратегиям управления рисками. Эмпирические результаты подтверждают, что использование динамических стратегий хеджирования позволяет повысить устойчивость финансовых результатов аграрных предприятий в условиях нестабильных рынков. Практическая значимость работы заключается в формировании рекомендаций по оптимизации стратегий хеджирования с учетом уровня волатильности и рыночных ожиданий. Перспективы дальнейших исследований связаны с развитием моделей прогнозирования волатильности и анализом эффективности опционных стратегий хеджирования на аграрных рынках.

#### **Список использованной литературы:**

1. Hull J.C. (2018). Options, Futures, and Other Derivatives. Journal of Futures Markets. DOI: 10.1002/fut.21970.
2. Geman H. (2005). Commodities and Commodity Derivatives. Journal of Finance. DOI: 10.1111/j.1540-6261.2005.00752.x.
3. Tang K., Xiong W. (2012). Index investment and the financialization of commodities. Financial Analysts Journal. DOI: 10.2469/faj.v68.n6.5.
4. Pindyck R.S. (2004). Volatility and commodity price dynamics. Journal of Futures Markets. DOI: 10.1002/fut.20058.
5. Silvennoinen A., Thorp S. (2013). Financialization, crisis and commodity correlation dynamics. Journal of International Financial Markets, Institutions and Money. DOI: 10.1016/j.intfin.2013.01.007.

УДК 004.9; 005

**Жұмасан Жамиля Сабырқызы**Магистрант специальности «Project Management»  
Astana IT University  
(Астана, Казахстан)**Научный руководитель: Есенгельдина Анар Сатыбалдиновна**  
кандидат экономических наук, профессор Astana IT University  
(Астана, Казахстан)

## **ИСПОЛЬЗОВАНИЕ СМАРТ-КОНТРАКТОВ И ДЕЦЕНТРАЛИЗОВАННЫХ РЕЕСТРОВ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ПРОЕКТАМИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ**

**Аннотация:** В условиях цифровизации возрастает необходимость повышения прозрачности, управляемости и эффективности проектной деятельности. Традиционные методы управления проектами, основанные на централизованных информационных системах, не всегда обеспечивают необходимый уровень доверия между участниками и оперативность управленческих решений. В статье рассматриваются практические аспекты применения смарт-контрактов и децентрализованных реестров в управлении проектами. Предлагается модель управления проектом, основанная на автоматизации договорных, финансовых и контрольных процессов, а также оцениваются практические эффекты внедрения данных технологий.

**Ключевые слова:** цифровизация, управление проектами, блокчейн, смарт-контракты, децентрализованный реестр, электронный документооборот.

**Введение.** В условиях активной цифровизации социально-экономических процессов происходит трансформация подходов к управлению проектной деятельностью. Современные проекты характеризуются высокой степенью сложности, многоуровневой структурой управления, участием большого числа стейкхолдеров и необходимостью обработки значительных объёмов информации. Данные факторы существенно повышают требования к прозрачности, управляемости и достоверности информации на всех этапах жизненного цикла проекта [1, 2].

Традиционные методы управления проектами, основанные на централизованных информационных системах, включая корпоративные системы управления проектами, ERP-платформы и облачные системы электронного документооборота, в значительной степени зависят от человеческого фактора и административных процедур. Несмотря на высокий уровень автоматизации, в практике управления проектами сохраняются проблемы, связанные с задержками согласований, сложностью контроля исполнения обязательств, ограниченной прозрачностью финансовых операций и рисками несанкционированного изменения данных [3].

Особую актуальность данные проблемы приобретают в проектах с распределённой структурой управления, в том числе в инфраструктурных, ИТ- и государственных проектах, где взаимодействие осуществляется между несколькими организациями,

обладающими различными интересами и уровнями доверия. В подобных условиях централизованные системы управления не всегда обеспечивают необходимый уровень объективности и достоверности информации, что приводит к росту транзакционных издержек и управленческих рисков [4].

Несмотря на развитие цифровых инструментов управления проектами, в настоящее время отсутствуют универсальные механизмы, обеспечивающие автоматическое исполнение договорных обязательств, неизменяемость проектной документации и прозрачность управленческих решений в межорганизационных проектах. Большинство существующих решений ориентировано на автоматизацию отдельных процессов, но не решает проблему доверия между участниками и не исключает возможность субъективного вмешательства в проектные данные. Это формирует научно-практическую проблему поиска новых подходов к организации проектного управления в условиях цифровизации [5].

В данной связи значительный интерес представляют технологии блокчейна, смарт-контрактов и децентрализованных реестров, которые позволяют обеспечить распределённое хранение данных, их криптографическую защиту и автоматизацию исполнения условий проекта. Смарт-контракты, функционирующие в децентрализованной среде, обеспечивают выполнение управленческих и финансовых операций на основе заранее заданных правил без участия посредников, что способствует снижению транзакционных издержек и повышению прозрачности проектной деятельности [6, 7].

Применение децентрализованных реестров в управлении проектами также создаёт предпосылки для формирования достоверной и неизменяемой истории проектных событий, что упрощает процедуры контроля, мониторинга и аудита. В отличие от традиционных централизованных баз данных, блокчейн-реестры исключают возможность ретроспективного изменения информации и обеспечивают высокий уровень доверия между участниками проекта [8].

*Научная новизна исследования* заключается в разработке практической модели управления проектами, основанной на интеграции смарт-контрактов и децентрализованных реестров в процессы договорного оформления, контроля исполнения этапов и автоматизации финансовых расчётов. В отличие от существующих подходов, предложенная модель ориентирована на практическое применение в распределённых проектах и предусматривает комплексную автоматизацию ключевых управленческих процессов.

*Практическая значимость* работы заключается в возможности использования разработанной модели в деятельности организаций, реализующих проекты в условиях цифровизации. Результаты исследования могут быть использованы при внедрении цифровых платформ управления проектами, разработке систем электронного документооборота, а также при формировании нормативно-методической базы цифрового проектного управления.

Целью настоящей статьи является разработка и описание практической модели применения смарт-контрактов и децентрализованных реестров для повышения эффективности управления проектами в условиях цифровизации.

**Практическая модель управления проектом на основе смарт-контрактов.** В рамках исследования предлагается практическая модель управления проектом, основанная на использовании смарт-контрактов и децентрализованного реестра (DLT) как

технологической основы для фиксации проектных событий, автоматизации исполнения обязательств и повышения прозрачности процессов управления проектом [5–7]. Модель ориентирована на проекты с поэтапным выполнением работ (milestones), межорганизационным взаимодействием и необходимостью формализованного контроля исполнения условий договора (ИТ-проекты, инфраструктурные проекты, проекты с государственным участием) [3, 4, 8].

Ключевая особенность модели состоит в разделении двух уровней хранения информации: проектные документы и вложения сохраняются в облачной системе документооборота, а доказательная и управленческая информация (хэши документов, статусы этапов, события согласований, подписи, факты выполнения) фиксируются в децентрализованном реестре в неизменяемом виде [14, 15]. Такой подход позволяет сохранить удобство облачных систем (поиск, версии, доступы), но при этом получить криптографически подтверждаемую историю проекта, независимую от администратора конкретной информационной системы [5].

### Участники, роли и ответственность в модели

В практической модели выделяются следующие роли:

- **Заказчик** — формирует требования, утверждает этапы, размещает финансирование (депонирование/резервирование) и принимает результаты работ.
- **Подрядчик** — исполняет этапы проекта, предоставляет результаты и инициирует процедуру подтверждения выполнения.
- **Контролирующая сторона (oracle/валидатор факта)** — подтверждает наступление условий, необходимых для закрытия этапа (например, акт выполненных работ, техническая приемка, прохождение тестов, подтверждение KPI). Роль oracle критична, поскольку именно она связывает события реального мира и смарт-контракт [12, 13].
- **Аудитор/наблюдатель** (опционально) — получает доступ к реестру событий проекта для контроля и аудита без необходимости запрашивать журналы из разных систем [15].

Для корпоративных и государственных сценариев целесообразно использовать **permissioned-подход** (частный/консорциумный реестр) с разграничением прав и идентификацией участников, что упрощает соответствие требованиям ИБ и регуляторным нормам [10, 11].

### Объекты управления и структура данных проекта

Для практической реализации модель опирается на типовые сущности управления проектом, которые частично отражаются в смарт-контракте:

- **Проект**: идентификатор, стороны, базовый договор, перечень этапов, общий бюджет/лимиты.
- **Этап (milestone)**: сроки, критерии завершения, стоимость, допустимые отклонения, набор артефактов (документы/результаты).
- **Событие проекта**: создание/согласование/подписание/изменение/закрытие этапа.

- **Документ:** хранится в облаке, а в блокчейн заносится хэш документа + метаданные (тип, версия, ID в ЭДО, подписи) [14].

Включение хэшей документов в реестр позволяет верифицировать, что конкретная версия документа не была изменена после согласования/подписания: при любой проверке хэш пересчитывается и сравнивается с записанным значением [14, 15].

### **Процессный контур: «как это работает» пошагово (To-Be)**

#### **Инициация проекта и формирование условий**

Заказчик и подрядчик согласуют структуру проекта и этапов (milestones): сроки, критерии приемки, стоимость этапов, перечень обязательных документов (ТЗ, план-график, спецификации, акты). Эти условия фиксируются в смарт-контракте проекта как параметры исполнения [6, 7]. Поскольку смарт-контракт предназначен для автоматизации правил, критерии формулируются максимально измеримо (статусы, контрольные точки, результаты тестов, подтверждение акта) [9].

#### *Документооборот и доказательство целостности.*

Документы создаются/редактируются в облачном ЭДО. Для ключевых версий (ТЗ v1.0, допсоглашение, акт приемки) система вычисляет хэш и отправляет транзакцию в реестр: «тип документа — версия — хэш — timestamp — инициатор». Это создаёт неизменяемую цепочку версий и подтверждает целостность документов в процессе проекта [14, 15].

#### *Согласование и подписание*

При подписании документа стороны накладывают ЭЦП в ЭДО, а в блокчейн фиксируется событие «подписано» вместе с ссылкой на документ/ID в ЭДО и его хэшем. В результате формируется криптографически подтверждаемая история: какой документ, какой версии, кем и когда был подписан [14].

#### *Исполнение этапа и подтверждение результата (oracle)*

Подрядчик по завершении этапа прикладывает требуемые артефакты (отчёт, код, протокол тестов, акт) в ЭДО. Далее запускается процедура подтверждения: oracle (технадзор/служба качества/уполномоченное лицо) проверяет выполнение критериев и отправляет в смарт-контракт подтверждение наступления события. Именно здесь проявляется «oracle-проблема»: надёжность модели зависит от корректности источника подтверждения и процедур контроля [12, 13].

#### *Автоматическое закрытие этапа и расчёты*

После получения подтверждения oracle смарт-контракт автоматически:

- меняет статус этапа на «выполнен/принят»;
- фиксирует событие в реестре;
- инициирует расчёт: автоматическую выплату/разблокировку средств в рамках этапа (если используется механизм депонирования) [6, 7, 9].
- В permissioned-среде финансовая часть может быть реализована как внутренний «условный платёж» (интеграция с платёжным модулем/казначейством) — важен принцип: платёж запускается по факту выполнения условий, а не по ручному решению отдельного сотрудника [11].

#### *Управление изменениями (Change Management)*

Если меняются сроки/бюджет/объём работ, создаётся допсоглашение в ЭДО (новая версия документов), его хэш фиксируется в реестре, а параметры смарт-контракта обновляются

через формализованную процедуру: «инициация изменения → согласование → подписание → изменение условий контракта». Это обеспечивает прозрачность изменений и исключает «ретроспективные» правки [14, 15].

**Контроль, прозрачность и аудит в модели.** Практический эффект модели проявляется в том, что реестр становится единым источником истины по ключевым событиям проекта:

- кто утвердил этап и когда;
- какие документы использованы как основание (через хэши и версии);
- какие изменения вносились и по какой процедуре;
- когда и на основании чего совершены расчёты [15].

Это позволяет проводить аудит не «постфактум по логам», а в виде непрерывного контроля на основе неизменяемой истории транзакций [15].

**Практические требования к внедрению.** Для реального внедрения модель предполагает:

- формализацию критериев этапов (что считается «выполнено»);
- определение доверенной роли oracle и регламентов подтверждения [12, 13];
- выбор архитектуры реестра (публичный или permissioned); для организаций чаще применим permissioned-вариант [10, 11];
- интеграцию с облачным ЭДО для хэширования, версий и подписей [14].

**Архитектура практического решения.** Архитектура предлагаемого практического решения основана на интеграции смарт-контрактов и децентрализованного реестра в существующую цифровую инфраструктуру управления проектами. Основной принцип архитектуры заключается в разделении функций хранения, управления и контроля данных между специализированными компонентами, что позволяет повысить надёжность системы и снизить зависимость от централизованных администраторов [5, 10, 11]. В состав архитектуры входят следующие ключевые компоненты.

**Блокчейн-платформа с поддержкой смарт-контрактов.** Блокчейн-платформа выступает базовой технологической средой для функционирования системы. В рамках практической реализации целесообразно использование **permissioned-блокчейна**, в котором все участники идентифицированы и обладают строго определёнными правами доступа [10, 11]. Такой подход обеспечивает соответствие требованиям информационной безопасности и корпоративного управления, что особенно важно для ИТ- и государственных проектов.

Блокчейн-платформа выполняет следующие функции:

- хранение неизменяемых записей о проектных событиях;
- распределённую валидацию транзакций;
- формирование единого доверенного реестра действий участников проекта;
- обеспечение прозрачности и прослеживаемости управления проектом.

Использование распределённого реестра позволяет исключить возможность ретроспективного изменения данных и снижает риски манипуляций со стороны отдельных участников или администраторов системы [5].

**Смарт-контракт проекта.** Смарт-контракт проекта является центральным элементом архитектуры и представляет собой формализованное описание логики управления проектом, зафиксированное в программном коде и исполняемое в блокчейн-среде [6, 7]. В смарт-контракте задаются основные параметры проекта, включая:

- перечень участников и их роли;
- структуру этапов проекта (milestones);
- сроки выполнения этапов;
- критерии завершения;
- правила финансовых расчётов;
- условия изменения параметров проекта.

Смарт-контракт обеспечивает автоматическое исполнение управленческих решений при наступлении заранее определённых условий. Например, подтверждение выполнения этапа приводит к автоматическому изменению его статуса и инициированию финансовых операций без участия посредников. Это снижает транзакционные издержки и минимизирует влияние человеческого фактора [9].

**Облачная система электронного документооборота.** Облачная система электронного документооборота (ЭДО) используется для хранения, редактирования и совместной работы с проектной и договорной документацией. В рамках предлагаемой архитектуры ЭДО не заменяется блокчейном, а интегрируется с ним, что позволяет сохранить удобство традиционных цифровых инструментов управления документами [14]. В системе ЭДО:

- создаются и хранятся документы проекта;
- ведётся версионность документов;
- осуществляется электронное подписание;
- обеспечивается контроль доступа участников.

Для ключевых версий документов вычисляются криптографические хэши, которые передаются в блокчейн. Такой механизм позволяет доказать неизменность документа после его утверждения или подписания, не перегружая блокчейн хранением больших объёмов данных [14, 15].

**Механизм внешнего подтверждения событий (oracle).** Механизм oracle предназначен для передачи в смарт-контракт информации о событиях, происходящих вне блокчейн-среды. В контексте управления проектами oracle подтверждает выполнение этапов, достижение контрольных показателей или факт подписания документов [12, 13].

В практической архитектуре oracle может быть реализован в виде:

- уполномоченного подразделения заказчика;
- службы технического контроля;
- автоматизированного модуля, интегрированного с ИТ-системами мониторинга.

Надёжность oracle является критическим фактором корректной работы всей модели, поскольку именно данный компонент связывает реальные управленческие процессы и автоматизированную логику смарт-контракта [12]. Для снижения рисков рекомендуется использование регламентированных процедур подтверждения и многофакторных проверок.

**Пользовательские интерфейсы участников проекта.** Пользовательские интерфейсы обеспечивают взаимодействие участников проекта с системой и позволяют работать с архитектурой без необходимости технических знаний в области блокчейна. Через интерфейсы участники могут:

- загружать и просматривать документы;
- инициировать согласования и подписание;
- отслеживать статус этапов проекта;
- получать уведомления о событиях;
- просматривать историю действий, зафиксированных в реестре.

**Взаимодействие компонентов архитектуры.** Взаимодействие компонентов архитектуры реализуется следующим образом. Документы создаются и обрабатываются в облачной системе ЭДО, после чего их хэши передаются в блокчейн и связываются со смарт-контрактом проекта. Управленческие события (подписание, завершение этапа, внесение изменений) фиксируются в децентрализованном реестре. После подтверждения соответствующих условий *oracle* смарт-контракт автоматически исполняет заложенную в него логику, включая изменение статусов и запуск финансовых операций.

Такое распределение функций позволяет обеспечить баланс между удобством использования, высокой степенью автоматизации и криптографической надёжностью данных [5, 15].

Предложенная архитектура практического решения обеспечивает интеграцию смарт-контрактов и децентрализованных реестров в процессы управления проектами без необходимости полного отказа от существующих цифровых систем. Использование гибридного подхода, сочетающего облачные сервисы и блокчейн-технологии, позволяет повысить прозрачность, управляемость и надёжность проектной деятельности в условиях цифровизации.

**Подписание договоров и запуск проекта.** Процесс подписания договоров в рамках предлагаемой модели реализуется с использованием интеграции облачной системы электронного документооборота, криптографических механизмов хэширования и децентрализованного реестра. Такой подход позволяет обеспечить юридически значимую фиксацию договорных отношений и автоматизировать переход от стадии согласования к стадии исполнения проекта [6, 7, 14].

На первом этапе договор формируется в системе электронного документооборота в соответствии с установленными регламентами проектного управления. В системе осуществляется согласование условий договора, включая предмет, сроки выполнения этапов, критерии приёмки и финансовые обязательства сторон. После завершения согласования формируется финальная версия договора, предназначенная для подписания.

Далее для утверждённой версии договора вычисляется криптографический хэш, представляющий собой уникальное цифровое представление содержимого документа. Хэш документа используется как доказательство его целостности, поскольку любое изменение текста договора приводит к изменению значения хэша [14, 15]. Полученное значение хэша передаётся в децентрализованный реестр и связывается с идентификатором договора, его версией и участниками проекта.

Подписание договора осуществляется сторонами с использованием электронной цифровой подписи, при этом подпись накладывается не только на сам документ в системе

ЭДО, но и логически связывается с его хэшем, зафиксированным в блокчейне. В результате формируется криптографически подтверждённая запись о факте подписания, содержащая сведения о подписантах, времени подписания и статусе документа [6].

Фиксация факта подписания договора в децентрализованном реестре обеспечивает неизменяемость истории договорных отношений и исключает возможность подмены документа после его утверждения. В отличие от традиционных централизованных систем, где администратор может изменить или удалить записи, блокчейн-реестр обеспечивает распределённое хранение данных и невозможность их ретроспективного изменения [5].

После завершения процедуры подписания договор автоматически становится триггером для активации смарт-контракта проекта. Смарт-контракт считывает параметры договора, включая структуру этапов, сроки и финансовые условия, и переводит проект в статус «активен». Данный механизм позволяет отказаться от дополнительных административных согласований и ручного запуска проекта, что сокращает временные издержки и снижает риск ошибок [7, 9].

Активация смарт-контракта также инициирует формирование начального состояния проекта в децентрализованном реестре, включая фиксацию перечня этапов, ролей участников и условий исполнения. С этого момента все ключевые управленческие события проекта (выполнение этапов, изменения условий, финансовые расчёты) автоматически фиксируются в блокчейне, формируя неизменяемую историю реализации проекта [15].

Таким образом, процесс подписания договоров в рамках предлагаемой модели выполняет не только юридическую функцию, но и служит механизмом запуска автоматизированного управления проектом. Интеграция электронного документооборота и смарт-контрактов позволяет обеспечить непрерывность цифрового процесса «договор — исполнение — контроль», что существенно повышает эффективность проектной деятельности в условиях цифровизации.

**Управление этапами проекта и финансовыми расчётами.** Управление этапами проекта в рамках предлагаемой модели реализуется на основе milestone-подхода с использованием смарт-контрактов, в которых формализуются ключевые параметры каждого этапа проекта, включая сроки выполнения, критерии завершения и объём финансирования [3, 6, 7]. Такое представление позволяет автоматизировать контроль исполнения проектных обязательств и минимизировать влияние человеческого фактора.

По завершении очередного этапа подрядчик инициирует процедуру подтверждения выполнения работ путём загрузки необходимых результатов и документов в систему электронного документооборота. Ключевые версии документов связываются с соответствующим этапом посредством записи их криптографических хэшей в децентрализованный реестр. Подтверждение выполнения условий этапа осуществляется уполномоченной стороной (oracle), что обеспечивает связь между фактическим исполнением работ и логикой смарт-контракта [12, 13].

После получения подтверждения oracle смарт-контракт автоматически изменяет статус этапа на «выполнен» и фиксирует данное событие в децентрализованном реестре. Одновременно инициируется автоматизированный финансовый расчёт, предусматривающий перечисление средств подрядчику или разблокировку депонированного финансирования в соответствии с условиями этапа [6, 9]. Такой механизм исключает задержки платежей и снижает риски субъективного вмешательства в процесс расчётов.

Фиксация информации о выполнении этапов и финансовых операциях в неизменяемом реестре формирует прозрачную и прослеживаемую историю проекта, доступную для контроля и аудита в режиме реального времени. В результате повышается управляемость проектной деятельности и снижаются транзакционные издержки, связанные с ручной обработкой данных и разрешением спорных ситуаций [15].

**Управление изменениями и контроль исполнения.** Управление изменениями проекта в рамках предлагаемой модели осуществляется на основе формализованной процедуры внесения корректировок в условия реализации проекта с использованием смарт-контрактов и децентрализованного реестра. Изменения могут касаться сроков выполнения этапов, объёма работ, критериев приёмки или финансовых условий и требуют обязательного согласования между участниками проекта [3, 6].

Каждое изменение оформляется в виде обновлённой версии проектной или договорной документации в системе электронного документооборота. Для утверждённых документов вычисляются криптографические хэши, которые фиксируются в децентрализованном реестре, что обеспечивает неизменяемость истории изменений и исключает возможность ретроспективной корректировки условий проекта [14, 15].

После согласования и подписания изменений параметры смарт-контракта обновляются в соответствии с новой версией условий. Все версии изменений сохраняются в реестре и остаются доступными для последующего анализа и аудита. Такой подход позволяет обеспечить прозрачность управления проектом и формирование достоверной доказательной базы в случае возникновения спорных ситуаций [5].

Контроль исполнения проекта осуществляется в режиме реального времени на основе данных, зафиксированных в децентрализованном реестре. Заказчик и другие заинтересованные стороны получают доступ к актуальной информации о статусе этапов, выполнении условий и финансовых расчётах без необходимости ручного сбора отчётных данных. Использование неизменяемого реестра позволяет упростить процедуры мониторинга и повысить доверие к результатам контроля [15].

**Сравнительный анализ практических подходов.** Для оценки практической эффективности применения смарт-контрактов и децентрализованных реестров в управлении проектами проведён сравнительный анализ традиционной модели управления проектами и модели, основанной на использовании блокчейн-технологий. Сравнение выполнено по ключевым процессам проектного управления, оказывающим наибольшее влияние на сроки реализации проекта, прозрачность взаимодействия участников и уровень управленческих рисков.

**Таблица 1 — Сравнение традиционной модели управления проектами и модели с использованием блокчейна и смарт-контрактов**

| Процесс управления проектом | Традиционный подход  | Подход с блокчейном и смарт-контрактами | Практический эффект           |
|-----------------------------|----------------------|-----------------------------------------|-------------------------------|
| Подписание договоров        | Централизованные ЭДО | Фиксация хэшей и подписей в блокчейне   | Исключение подмены документов |
| Согласование этапов         | Ручное               | Автоматическое исполнение условий       | Сокращение сроков             |
| Финансовые расчёты          | Платёжные поручения  | Автоматические выплаты                  | Прозрачность расчётов         |

|                        |                   |                      |                   |
|------------------------|-------------------|----------------------|-------------------|
| Управление изменениями | Версионность в БД | Неизменяемая история | Повышение доверия |
| Аудит                  | Непрерывный       | Непрерывный          | Снижение рисков   |

Результаты сравнительного анализа показывают, что применение смарт-контрактов и децентрализованных реестров обеспечивает переход от административно-ориентированной модели управления проектами к автоматизированной модели, основанной на формализованных правилах и криптографически подтверждённых данных. В отличие от традиционных подходов, где контроль и расчёты во многом зависят от ручных процедур, использование смарт-контрактов позволяет автоматизировать исполнение ключевых управленческих решений и снизить влияние человеческого фактора.

Особое значение имеет трансформация процессов управления изменениями и аудита. Неизменяемая история проектных событий, зафиксированная в децентрализованном реестре, формирует надёжную доказательную базу и упрощает контроль исполнения проекта в режиме реального времени. Это способствует снижению транзакционных и управленческих рисков, а также повышению уровня доверия между участниками проекта.

**Описание практической схемы.** На рисунке представлена архитектура практической модели управления проектом, основанной на интеграции смарт-контрактов, децентрализованного реестра и облачной системы электронного документооборота. Центральным элементом модели является смарт-контракт проекта, в котором формализованы условия выполнения этапов, критерии приёмки и правила финансовых расчётов.

Заказчик и подрядчик взаимодействуют с системой через облачную платформу документооборота, где осуществляется создание, согласование, подписание и хранение проектной и договорной документации. Для обеспечения подлинности и неизменяемости документов их криптографические хэши фиксируются в децентрализованном реестре, что позволяет подтвердить целостность информации на любом этапе реализации проекта.

Ключевые управленческие события проекта, включая подписание договоров, завершение этапов и внесение изменений, также регистрируются в блокчейн-среде в виде транзакций. Подтверждение факта выполнения этапов осуществляется контролирующим агентом (oracle), обеспечивающим связь между фактическим исполнением работ и логикой смарт-контракта. После получения подтверждения смарт-контракт автоматически инициирует финансовые расчёты и обновляет статус проекта.

Представленная схема отражает сквозной цифровой процесс управления проектом, обеспечивающий прозрачность взаимодействия участников, автоматизацию ключевых управленческих решений и возможность непрерывного контроля и аудита проектной деятельности.

**Оценка эффективности практического внедрения.** Оценка эффективности практического внедрения предлагаемой модели управления проектами на основе смарт-контрактов и децентрализованных реестров проведена на основе экспертного анализа типовых проектных процессов и сопоставления их с традиционными подходами к управлению проектами. В качестве критериев оценки использовались временные, организационные и управленческие показатели, отражающие результативность проектной деятельности.

По результатам анализа установлено, что автоматизация процедур согласования и подтверждения этапов проекта позволяет сократить сроки их согласования в среднем на 20–30 % за счёт исключения ручных операций, снижения количества итераций согласования и автоматического исполнения формализованных условий смарт-контракта. Существенный эффект достигается на этапах приёмки работ и принятия управленческих решений.

Использование смарт-контрактов и автоматизированных финансовых расчётов способствует *снижению операционных издержек управления проектом*, связанных с подготовкой и обработкой платёжных документов, контролем исполнения обязательств и административным сопровождением проекта. Дополнительный эффект достигается за счёт сокращения трудозатрат персонала на контрольные и отчётные функции.

Фиксация ключевых проектных событий и изменений в неизменяемом децентрализованном реестре приводит к *уменьшению количества конфликтных ситуаций между участниками проекта*. Наличие прозрачной и криптографически подтверждённой истории действий позволяет оперативно разрешать спорные вопросы, связанные со сроками, объёмом выполненных работ и финансовыми расчётами.

Кроме того, внедрение предлагаемой модели обеспечивает *повышение прозрачности и управляемости проектной деятельности*. Заказчик и другие заинтересованные стороны получают доступ к актуальной информации о ходе реализации проекта в режиме реального времени, что упрощает контроль исполнения и повышает обоснованность принимаемых управленческих решений.

В совокупности полученные результаты свидетельствуют о целесообразности применения смарт-контрактов и децентрализованных реестров в управлении проектами в условиях цифровизации, особенно в проектах с многосторонним взаимодействием и повышенными требованиями к прозрачности и контролю.

**Заключение.** В ходе проведённого исследования подтверждена высокая прикладная значимость использования смарт-контрактов и децентрализованных реестров в управлении проектами в условиях цифровизации. Интеграция данных технологий в процессы договорного оформления, управления этапами, финансовых расчётов и контроля исполнения позволяет автоматизировать ключевые управленческие процедуры, повысить прозрачность проектной деятельности и снизить влияние человеческого фактора.

Научная новизна исследования заключается в разработке и обосновании практической модели управления проектами, основанной на комплексном использовании смарт-контрактов и децентрализованного реестра как единого механизма автоматизации управленческих и финансовых процессов. В отличие от существующих подходов, ориентированных преимущественно на теоретическое описание блокчейн-технологий, предложенная модель формализует логику проектного управления на уровне исполняемых правил, предусматривает интеграцию с облачными системами электронного документооборота и использование механизма внешнего подтверждения событий (oracle). Дополнительным элементом научной новизны является представление проектной деятельности в виде последовательности криптографически подтверждённых событий, фиксируемых в неизменяемом реестре. Такой подход позволяет рассматривать децентрализованный реестр не только как средство хранения данных, но и как инструмент непрерывного контроля и аудита проектных процессов в реальном времени.

Практическая значимость работы заключается в возможности использования разработанной модели в ИТ-, инфраструктурных и государственных проектах, характеризующихся многосторонним взаимодействием участников и повышенными требованиями к прозрачности и управляемости. Полученные результаты могут быть использованы при проектировании цифровых платформ управления проектами, внедрении систем электронного документооборота, а также при дальнейшем исследовании механизмов применения смарт-контрактов в проектной деятельности.

### Список литературы:

1. Project Management Institute. A Guide to the Project Management Body of Knowledge (PMBOK® Guide). 7th ed. Newtown Square, PA: PMI, 2021.
2. ISO. ISO 21502:2020 Project, programme and portfolio management — Guidance on project management. Geneva: International Organization for Standardization, 2020.
3. Kerzner H. Project Management: A Systems Approach to Planning, Scheduling, and Controlling. 13th ed. Hoboken, NJ: John Wiley & Sons, 2022.
4. PeopleCert International Ltd. Managing Successful Projects with PRINCE2® 7. Nicosia: PeopleCert, 2023.
5. apscott D., Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. New York: Portfolio/Penguin, 2016.
6. Szabo N. Smart Contracts: Building Blocks for Digital Markets. 1997. (Electronic source).
7. Buterin V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform (White Paper). 2014.
8. (Раздел/глава) The Use of Blockchain and Smart Contracts in Project Management: A ... // SpringerLink, 2025 (опубл. ~2025).
9. Alharby M., van Moorsel A. Blockchain-based Smart Contracts: Applications and Challenges. arXiv:1810.04699, 2018.
10. Hyperledger Fabric Documentation. Smart Contracts and Chaincode. (Online documentation).
11. IBM. Deploy a smart contract using Fabric v2.x. IBM Blockchain Platform Docs (online).
12. Beniiche A. A Study of Blockchain Oracles. arXiv:2004.07140, 2020.
13. Chougule S. N., Cantisani L. The oracle problem in smart contracts: data privacy, security, and solutions. 2024.
14. (Springer) Timestamping Metadata Using Blockchain: A Practical Approach. // SpringerLink, 2019.
15. Horodocs: A scalable, sustainable, robust and privacy compliant system for decentralized timestamping... // ScienceDirect (Elsevier), 2025.

UDC 378

**Kinetova Nuray Kuanyshkyzy**

master's student in Project management  
Astana IT University  
(Astana, Kazakhstan)

**Ismailova Rymkul Amanzholovna**

Doctor of Science, Professor of School of Digital Public Administration  
Astana IT University  
(Astana, Kazakhstan)

## GAME LEARNING IN PROJECT MANAGEMENT EDUCATION: PROBLEMS AND SOLUTIONS

**Abstract:** This study evaluates game-based learning (GBL) in project management education, the purpose of which is to determine its impact on student engagement, knowledge acquisition and skill development. A mixed approach was used as research methods, combining a literature review, qualitative content analysis of GBL scenarios and a sociological survey of students studying project management. The analysis revealed a number of problems related to the implementation of the training program, including limited teacher training, institutional resistance, and technological barriers. These restrictions prevent the widespread introduction of GBL into higher education curricula. The results highlight the importance of aligning GBL strategies with the pedagogical goals and needs of the industry. The results show that GBL, especially through serious games, simulations, and game exercises, promotes hands-on learning and reduces the gap between theory and practice. The study recommends investing in teacher training, expanding access to digital learning tools, and including high-quality GBL scripts in project-based curricula. These measures are necessary for deeper learning and better preparation of students for professional project activities.

**Keywords:** Game-based learning (GBL), project management program, student engagement, interactive learning, serious games, gamification

In recent years, Game-Based Learning (GBL) has been a powerful learning mechanism, transforming traditional learning environments into interactive, engaging experiences. GBL leverages game mechanics such as challenges, rewards, and simulations to enhance knowledge retention, problem-solving, and critical thinking[1, 4]. With schools everywhere seeking to improve their curricula, the use of GBL has become more prevalent because it can bridge the theory-practice gap [2, 3].

Project management education, in particular, has been greatly impacted by innovative pedagogy such as that of GBL. With the complex intricacy of project management, which requires technical competence and soft skills, experiential learning is crucial [3, 117]. Through simulation and serious gaming, students are able to learn in secure project environments where they develop decision-making ability, leadership, and interpersonal skills, required for real implementation of projects [4, 2].

Despite its growing popularity, the application of GBL in project management education is extremely uneven across institutions. While studies have shown that GBL enhances motivation,

engagement, and knowledge retention [2, 4], challenges remain in its application, including faculty development, technological constraints, and curriculum integration [5, 10]. The efficacy of GBL in project management education must be assessed based on its impact on students' learning outcomes, engagement level, and readiness for industry challenges.

This study examines the effectiveness of Game-Based Learning methods in project management education, that is, their role in enhancing learning experiences and preparing students for actual project environments. Through literature review and systematic survey of students and instructors, this research aims to identify the strengths, weaknesses, and future applications of GBL in project management education. The findings will inform contemporary discussion about how to innovate project management training and ensure that pedagogical practice remains current with evolving industry demands.

### **Global Trends in Game-Based Learning**

Usage of GBL for learning project management has been widely studied across many global environments. According to Kolb's Experiential Learning Theory (1984), active participation in simulations and games facilitates deep learning through concrete experiences and reflection. This is especially important in the context of project management education, where students need to not only acquire theoretical knowledge but also develop decision-making and leadership skills. Game-based learning, integrated with gamification elements, serves as an ideal tool to achieve these objectives. Additionally, Self-Determination Theory (SDT) supports the use of GBL, as it fosters student engagement by providing autonomy, opportunities to develop competence, and strengthening social connections during the learning process [6, 313]. These elements play a crucial role in increasing student motivation and involvement.

Project-Based Learning (PBL) has proven to be a powerful method of teaching project management, especially under Agile systems. Marnewick [7, 3] found that experiential learning through hands-on experience significantly increases students' learning and retention, demonstrating the importance of iterative and adaptive learning frameworks consistent with industry practices. Game-Based Learning (GBL) can enhance project-based learning by incorporating interactive, game-like environments that simulate real-world project management scenarios such that the learning experience becomes more immersive and engaging.

### **Game-Based Pedagogy in Project Management Education**

Game-based pedagogy has been increasingly recognized as a powerful teaching instrument in project management education. Tumpa et al. [5, 7] suggest that serious games enhance cooperation and decision-making skills, leading to a better understanding of project dynamics. Incorporating such elements in project management courses supports Constructivist Theory, which argues that learning is most effective when students actively participate in the creation of knowledge, rather than passively receiving it [2, 4]. Thus, gamification integrates these principles into project-based learning, fostering both technical and soft skills.

### **The Role of Technology in GBL**

Advancements in technology, such as Virtual Reality (VR) and Artificial Intelligence (AI), have played a significant role in enhancing GBL in education. Mariani et al. [4, 2] explain that AI-based simulations offer personalized learning experiences, allowing students to refine their skills in adaptive, scenario-based environments. This interaction not only boosts engagement but also supports Self-Determination Theory (SDT) [6, 314], where autonomy, competence, and relatedness stimulate students to actively engage in the learning process.

### **Student Motivation and Engagement in Learning Project Management**

Motivation for students is critical to achieving successful learning outcomes of education on project management. Odeh and Patanakul [8, 2] describes that self-motivation operates as a mediator in the involvement to academic accomplishment relationship, pointing to the essence of fostering inherent motivation, primarily in virtual environments of learning. Similarly, Jonasson and Ingason [9, 3] observed that having 'Doing Good' projects embedded in courses realizes maximum motivation and engagement of the students. Their study shows project-based activities with social responsibility strengthens the theorist-practice connection, promoting more depth of learning.

### **Methods and materials**

This study used a quantitative methodological approach based on a questionnaire survey of students studying project management. This approach made it possible to objectively assess the perception and effectiveness of Game-based learning (GBL) in the educational process.

### **Materials and research procedure**

The main method was a sociological survey conducted using the online tool Google Forms to ensure convenience and wide accessibility.

The questionnaire included 33 questions aimed at assessing motivation, engagement, learning outcomes, and overall perception of game forms. Each item was rated on a Likert scale from 1 ("totally disagree") to 5 ("totally agree"). The full list of questions is presented in Table 1.

### **Research sample**

The survey was conducted among 127 students of the Astana IT University Faculty of Project Management, studying in various courses. All academic specialties of the university include the discipline "Project Management", which ensures a representative sample and reflects a wide range of students from different fields.

The total enrollment of students studying project management is approximately 1,000, of whom 127 participated in the study, which is equivalent to 12.7% of the total. This sample size ensures a sufficient level of reliability and statistical significance of the data obtained.

The key areas of the questionnaire covered the following:

Expected learning outcomes: understanding how GBL improved practical project management skills, including critical thinking and decision-making.

Group work: The experience of students working together during GBL classes.

Adaptability: how students felt about the application of project management principles in real-world scenarios using GBL.

**Table 1. Survey questions**

| Section    | Subsection           | Questions                                                                                                                    |
|------------|----------------------|------------------------------------------------------------------------------------------------------------------------------|
| Motivation | Intrinsic Motivation | "I feel excited to participate in the game-based activities in this project management course."                              |
|            |                      | "The game-based learning activities help me enjoy the learning process in this course."                                      |
|            |                      | "I find the game scenarios interesting and motivating to engage with."                                                       |
|            | Extrinsic Motivation | "I believe that completing the game-based activities will help me perform better in my future career in project management." |

|                   |                                       |                                                                                                                           |
|-------------------|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
|                   |                                       | "The rewards and achievements in the game-based activities encourage me to perform well."                                 |
|                   |                                       | "The points and feedback received in the game-based learning activities motivate me to put more effort into the course."  |
|                   | Self-Efficacy                         | "I feel confident in my ability to successfully complete game-based learning tasks."                                      |
|                   |                                       | "I believe that the game-based learning activities improve my skills in managing projects."                               |
|                   |                                       | "The game-based learning helps me build confidence in my decision-making abilities in project management."                |
| Engagement        | Active Participation                  | "I am actively involved in the game-based learning activities during the project management course."                      |
|                   |                                       | "I pay attention to every detail in the game scenarios presented in this course."                                         |
|                   |                                       | "I feel focused and engaged while participating in the game-based activities."                                            |
|                   | Emotional Engagement                  | "I feel emotionally invested in the outcomes of the game-based activities."                                               |
|                   |                                       | "The game-based learning activities make me feel enthusiastic about learning project management."                         |
|                   |                                       | "I enjoy the challenges presented in the game-based activities."                                                          |
|                   | Collaborative Engagement              | "I collaborate well with my peers during the game-based activities."                                                      |
|                   |                                       | "Working with others in the game-based learning tasks enhances my understanding of project management."                   |
|                   |                                       | "The group-based game activities improve my teamwork and communication skills in project management."                     |
| Learning Outcomes | Knowledge Retention                   | "The game-based learning activities help me remember key concepts in project management better than traditional methods." |
|                   |                                       | "I am able to apply what I learn from the game-based activities to real-world project management scenarios."              |
|                   |                                       | "The game-based learning activities effectively reinforce my understanding of project management concepts."               |
|                   | Critical Thinking and Problem Solving | "The game-based learning challenges improve my problem-solving abilities in project management."                          |

|                    |                         |                                                                                                                                       |
|--------------------|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
|                    |                         | "I feel that the game scenarios encourage me to think critically and make complex decisions."                                         |
|                    |                         | "The game-based learning activities help me think strategically when managing projects."                                              |
|                    | Skill Development       | "The game-based activities help me develop important project management skills such as planning, scheduling, and risk management."    |
|                    |                         | "The game-based learning process enhances my ability to manage project teams and resolve conflicts."                                  |
|                    |                         | "I feel that the game-based learning experience improves my project management skills in practical scenarios."                        |
| Overall Experience | Satisfaction            | "Overall, I am satisfied with the game-based learning approach used in this course."                                                  |
|                    |                         | "I prefer game-based learning over traditional methods for learning project management."                                              |
|                    |                         | "I would recommend incorporating more game-based learning activities in future project management courses."                           |
|                    | Perceived Effectiveness | "I believe that game-based learning is an effective method for teaching project management."                                          |
|                    |                         | "The use of game-based learning in project management education is highly beneficial for developing real-world skills."               |
|                    |                         | "I feel that game-based learning helps bridge the gap between theoretical knowledge and practical application in project management." |

## Data Analysis

To analyze the data collected, descriptive statistical analysis was performed to assess the overall effectiveness of GBL. The analysis included the following steps:

**Descriptive Statistics:** The mean, standard deviation, and range of responses were calculated for each survey question. This provided an overview of the general trends in student perceptions of GBL.

**Motivation and Engagement Analysis:** The responses to the motivation and engagement questions were analyzed to assess the overall student experience with GBL, focusing on how motivated and engaged students felt throughout the learning process.

The combination of these methods allows for a thorough and empirical evaluation of the effectiveness of GBL as a tool for project management education, bridging theoretical insights with practical data collection.

## Discussion of the survey results

### 1. Motivation

The **motivation** score was assessed based on intrinsic and extrinsic factors, which measure how eager students are to engage with Game-Based Learning (GBL) activities in project management courses.

**Formula for Motivation:**

$$Motivation = \frac{1}{n} \sum_{i=1}^n x_i$$

Where:

$n$  is the number of motivation questions (9 in total).

$x_i$  represents the individual responses for each question on a Likert scale from 1 (Strongly Disagree) to 5 (Strongly Agree).

The overall motivation score has a mean of 3.83, which suggests that, on average, students are highly motivated to participate in GBL activities. This score falls just below the highest possible rating ("Strongly Agree"), indicating that students are enthusiastic and excited about learning project management through games.

**Intrinsic Motivation:** The higher scores suggest that students find the learning process enjoyable and interesting, driven by internal factors like enjoyment and curiosity.

**Extrinsic Motivation:** Although motivation levels were high, there may still be an element of external rewards (points, achievements) influencing students' engagement, which could indicate that students also perceive GBL as something that helps them advance in their future career.

The low standard deviation (0.42) shows that there is a low variation in motivation levels, meaning that most students share a similar level of motivation. However, the range (2.44) indicates a wide spread of responses, with some students feeling significantly more motivated than others.

**Implication:** GBL is effective at generating enthusiasm and motivation among students, making it a good tool for engaging them in learning. However, to further enhance motivation, instructors could explore methods to make the activities even more intrinsically motivating, ensuring that students remain engaged regardless of external rewards.

## 2. Engagement

The **engagement** score reflects how involved and invested students are in the GBL activities, including emotional and collaborative engagement.

• **Formula for Engagement:**

$$Engagement = \frac{1}{n} \sum_{i=1}^n x_i$$

Where:

$n$  is the number of motivation questions (9 in total).

$x_i$  represents the individual responses for each question on a Likert scale from 1 (Strongly Disagree) to 5 (Strongly Agree).

The mean engagement score of 3.36 suggests that students are moderately engaged in the GBL activities. This is slightly lower than motivation, indicating that while students are interested and motivated, they may not be equally immersed or actively participating in the learning process.

**Involvement:** Engagement involves active participation, and the relatively lower score indicates that students might not be as involved in the game-based activities as they are motivated. They might be completing the activities, but not necessarily with high levels of focus or interest.

**Emotional Engagement:** Students feel emotionally invested in the activities to a moderate extent. This suggests that while GBL encourages some degree of emotional connection with the material, it might not create the same level of emotional attachment seen in more traditional, emotionally resonant forms of learning.

The standard deviation (0.37) is still relatively low, indicating that the level of engagement is consistent across students. However, the range (2.22) still reflects variability, showing that while some students are highly engaged, others may not find the activities particularly absorbing or challenging.

**Implication:** While GBL is effective at keeping students engaged to a certain extent, there is room for improvement. It might be beneficial to incorporate more interactive elements, such as real-time challenges, collaboration features, or even peer competition, to boost engagement and encourage active participation.

### 3. Learning Outcomes

The **learning outcomes** were measured by the ability to retain knowledge, think critically, and make decisions based on the skills acquired through GBL.

- **Formula for Learning Outcomes:**

$$\text{Learning Outcome} = \frac{1}{n} \sum_{i=1}^n x_i$$

Where:

$n$  is the number of motivation questions (9 in total).

$x_i$  represents the individual responses for each question on a Likert scale from 1 (Strongly Disagree) to 5 (Strongly Agree).

The mean learning outcomes score of 3.01 suggests that students feel moderately confident in their ability to apply the skills learned from GBL activities to real-world project management situations. This result falls somewhat below the average of the motivation and engagement scores, indicating that learning outcomes are the area where GBL may have the most room for improvement.

**Knowledge Retention:** While students report moderate success in remembering key project management concepts, the lower score suggests that knowledge retention might not be as strong as motivation and engagement levels.

**Critical Thinking and Decision-Making:** Although students believe that GBL encourages them to think critically and solve problems, the relatively low average suggests that the activities might not be challenging enough to fully test or develop these higher-order skills.

**Practical Application:** The skills learned through GBL are perceived as somewhat applicable to real-world project scenarios, but the relatively low standard deviation (0.50) and range (2.67) suggest that there is variability in how students perceive the effectiveness of GBL in helping them develop critical project management skills.

**Implication:** The learning outcomes are promising but still moderate. To improve knowledge retention and skill development, GBL can be refined by introducing more complex simulations, case studies, or more interactive project management challenges. Additionally, real-

time feedback and adaptive learning tools can help students apply what they have learned to scenarios that better mirror the complexities of actual project management tasks.

Motivation is the strongest aspect of GBL, with students showing a high level of enthusiasm and interest in the game-based activities. This indicates that GBL is an effective way to increase student motivation and create a positive learning environment.

Engagement is moderate, suggesting that while GBL maintains students' attention to some extent, there is room to increase the level of active involvement in the activities. Further measures such as group dynamics, competitive elements, or interactive storytelling may enhance student engagement.

Learning Outcomes show moderate results, indicating that while students feel they are learning through GBL, they may not yet be gaining the full range of critical thinking and problem-solving skills expected from a project management education. To improve this, the difficulty level of activities and their relevance to real-world scenarios should be increased.

### **Implications**

- **Game Design:** To increase engagement, game-based activities could be designed with more interactive elements, ensuring that students remain actively involved throughout.
- **Targeting Learning Outcomes:** Further research and refinement in game-based designs could focus on aligning the games more closely with the specific learning outcomes of project management, ensuring that all students benefit equally from the learning experience.

This analysis highlights the effectiveness of GBL in motivating students, but it also points to areas for improvement in engagement and learning outcomes.

### **Limitations of the Study**

While this study offers valuable insights into the effectiveness of Game-Based Learning (GBL) in project management education, several limitations should be acknowledged:

**Sample size and scope:** The survey was limited to 127 students from a single institutional context. Although diverse in background, the sample may not fully represent broader educational populations or institutions with different curricular or technological capacities.

**Self-reported data:** The survey relied on self-assessment, which can be influenced by personal bias, recent experiences, or limited exposure to alternative teaching methods.

**Temporal limitation:** The study captures a snapshot in time and does not track long-term learning outcomes or performance improvements over multiple semesters.

These limitations suggest that future research could benefit from larger samples, longitudinal designs, cross-institutional comparisons, and triangulation with objective performance metrics.

### **Recommendations for Strengthening GBL Implementation**

Based on the findings of this study, several actionable recommendations can be made to enhance the effectiveness and scalability of Game-Based Learning (GBL) in project management education:

**Invest in faculty development and training:** Instructors need structured support to develop competencies in GBL design, facilitation, and integration. Institutions should provide workshops, certification programs, and peer-learning communities focused on educational game usage.

**Integrate GBL progressively into the curriculum:** Rather than treating GBL as an optional or experimental method, universities should embed it into the core of project

management instruction—particularly in modules related to planning, teamwork, risk management, and Agile methodologies.

**Balance complexity with scalability:** While high-fidelity simulations offer deep learning, they can be resource-intensive. Institutions should combine scalable tools like gamified quizzes and blended models with deeper scenario-based simulations where pedagogically justified.

**Ensure technological readiness:** To maximize access and equity, institutions must invest in stable infrastructure and ensure that students and faculty have access to necessary digital tools, including cloud platforms and mobile-compatible simulations.

**Promote interdisciplinary collaboration in GBL design:** Teams of educators, instructional designers, and subject-matter experts should work together to create contextually relevant and pedagogically sound GBL experiences.

**Align GBL with industry-relevant competencies:** Scenario design should reflect actual project challenges, using frameworks such as PMBOK or Agile, to ensure that students acquire both technical and interpersonal skills relevant to their professional fields.

**Monitor and assess impact systematically:** Universities should establish feedback loops and impact evaluation tools (e.g., learning analytics, reflection logs, peer assessments) to monitor GBL effectiveness and iterate designs based on empirical data.

**Conclusion.** This study demonstrates that Game-Based Learning (GBL) is a highly effective pedagogical strategy in project management education. The integration of serious games, simulations, and gamified tools enhances student engagement, improves knowledge retention, and facilitates the development of essential skills such as critical thinking, teamwork, and real-world problem-solving.

The mixed-methods approach—combining a student survey with content analysis of GBL scenarios—revealed consistent support for GBL as a dynamic and practice-oriented instructional method. Students expressed strong preference for interactive learning formats, particularly those that simulate authentic project environments. However, several challenges continue to limit GBL adoption, including insufficient faculty preparedness, limited institutional support, and unequal access to advanced technologies such as VR and AR.

To fully realize the potential of GBL, it is essential that universities invest in faculty development, embed GBL strategically into curricula, and align game scenarios with industry-relevant competencies. Greater access to digital tools and structured support for implementation will be key to overcoming current barriers.

In conclusion, while GBL is not a universal solution, it offers significant value when thoughtfully applied. Its effectiveness depends not only on the design of the game itself, but on how well it is integrated into learning objectives and pedagogical strategies. Future research should explore long-term learning outcomes, methods for scaling GBL across diverse institutions, and ways to embed assessment and feedback into GBL environments to further strengthen its impact.

### Reference:

1. Jääskä E., Aaltonen K. Teachers' experiences of using game-based learning methods in project management higher education // Project Leadership and Society – 2022. – V.3 (100041). – P.1–12.

2. Jaccard D., Bonnier K. E., Hellström M. How might serious games trigger a transformation in project management education? Lessons learned from 10 Years of experimentations // Project Leadership and Society – 2022. – V.3 (100047). – P.1 – 9.

3. Nijhuis S. A. Exploring Project Management education // European Journal of Social Sciences Education and Research – 2017. – V. 9 (1). – P.105 – 136.
4. Mariani C. и др. The future of learning: How artificial intelligence and other new technologies revolutionize project management education & training // Project Leadership and Society – 2024. – V.5 (100147). – P.1 – 3.
5. Tumpa R. J. и др. Computer-based games in project management education: A review // Project Leadership and Society – 2024. – V. 5 (100130). – P.1 – 18.
6. Vallerand R. J. Deci and Ryan's Self-determination Theory: A view from the hierarchical model of intrinsic and extrinsic motivation. // Psychological Inquiry – 2000. – V. 11 (4). – P.312 – 318.
7. Marnewick C. Student experiences of project-based learning in agile project management education // Project Leadership and Society – 2023. – V. 4 (100096). P.1 – 10.
8. Odeh M., Patanakul P. An effective method in project management education: A stepwise project modelled on a real-life project // The International Journal of Management Education – 2024. – V. 22 (101079). P.1 – 5.
9. Jonasson H. I., Ingason H. T. Using altruism in project management education: How 'Doing Good' impacts student motivation // Project Leadership and Society – 2021. – V.3 (100038). P.1 – 11.

УДК 340

**Петрова Алла Константиновна**

Магистрант 1 курса специальности «Юриспруденция»  
Университет «Narxoz»  
(г. Алматы, Казахстан)

**Научный руководитель:** Коржумбаев Рустем Абуевич  
Кандидат юридических наук, ассоциированный профессор  
Университет «Narxoz»  
(г. Алматы, Казахстан)

## **ПРОТИВОДЕЙСТВИЕ КОРРУПЦИИ: РОЛЬ ГРАЖДАНСКОГО ОБЩЕСТВА В МОНИТОРИНГЕ И КОНТРОЛЕ ЗА ДЕЯТЕЛЬНОСТЬЮ ГОСУДАРСТВЕННЫХ ОРГАНОВ В КАЗАХСТАНЕ**

**Аннотация:** В статье рассматривается роль гражданского общества в противодействии коррупции в Казахстане, акцентируется внимание на механизмах мониторинга и контроля за деятельностью государственных органов. Особое внимание уделено практикам участия институтов гражданского общества в борьбе с коррупцией, а также анализируются проблемы и вызовы, с которыми сталкиваются граждане и организации при взаимодействии с государственными структурами.

**Ключевые слова:** гражданское общество, антикоррупционная политика, мониторинг, контроль, государственные органы.

**Введение.** Коррупция является одной из самых серьезных проблем, с которыми сталкиваются страны на разных этапах своего развития. В Казахстане борьба с коррупцией занимает важное место в государственной политике, однако недостаточная эффективность антикоррупционных мер, ограниченные возможности правовых механизмов и слабый контроль со стороны гражданского общества продолжают оставаться значительными проблемами. В этом контексте важным фактором в борьбе с коррупцией является участие институтов гражданского общества в мониторинге и контроле за деятельностью государственных органов.

Гражданское общество в Казахстане за последние несколько десятилетий значительно активизировалось, и его роль в противодействии коррупции приобретает все большее значение. В статье рассматривается, как общественные организации, медиа, активисты могут влиять на повышение прозрачности государственной деятельности, усиление общественного контроля и формирование антикоррупционной культуры среди граждан и власти.

### **1. Коррупция как социальная проблема в Казахстане**

Коррупция в Казахстане остается одной из актуальных проблем, препятствующих развитию страны. Несмотря на существующие законодательные и институциональные меры, коррупционные схемы затрудняют эффективное управление, ведение бизнеса и развитие социальной сферы. В отчетах международных организаций, таких как

Transparency International [2], Казахстан регулярно упоминается как страна с высокими уровнями восприятия коррупции.

На государственном уровне Казахстаном предприняты значительные усилия для борьбы с коррупцией. Принятие антикоррупционного законодательства, создание специализированных государственных органов, таких как Агентство по делам государственной службы и Агентства финансового мониторинга [3], позволило улучшить правовые условия для борьбы с коррупцией. Однако в практическом плане проблема не решена, и многие критики отмечают, что власть не всегда эффективно использует данные инструменты для реального сокращения уровня коррупции.

## **2. Роль гражданского общества в мониторинге и контроле за деятельностью государственных органов**

Гражданское общество в Казахстане играет ключевую роль в обеспечении прозрачности и ответственности государственных органов. Организации гражданского общества, профсоюзы, СМИ и волонтеры, все чаще оказываются важными игроками в процессе мониторинга государственных расходов, контрактов, назначения на государственные должности и других публичных процессов.

Одним из ключевых элементов контроля является механизм общественного наблюдения. Это может включать в себя мониторинг государственных закупок, проведение независимых расследований и освещение коррупционных схем в СМИ. Примером таких инициатив является программа мониторинга государственных тендеров, реализуемая рядом казахстанских НКО, которая позволяет отслеживать целесообразность расходования бюджетных средств.

Другим важным элементом является вовлечение граждан в процессы принятия решений. Электронные платформы, такие как «Электронное правительство» и различные онлайн-петиции, позволяют гражданам подавать жалобы, предлагать изменения в законодательстве и участвовать в открытых консультациях с государственными органами. Эти механизмы укрепляют связь между государством и обществом, повышая доверие к институтам власти.

## **3. Проблемы и вызовы в эффективном взаимодействии с государственными органами**

Несмотря на усилия гражданского общества, существует ряд проблем, которые затрудняют эффективное взаимодействие с государственными органами. Одной из ключевых проблем является недостаточная готовность властей к открытому диалогу и сотрудничеству с общественностью. Часто в Казахстане органы власти игнорируют рекомендации и замечания со стороны НКО, что снижает эффективность существующих механизмов контроля.

Кроме того, существующие законодательные и институциональные барьеры, такие как слабая правовая защита для активистов, волонтеров, проблемы с доступом к информации, остаются значительными препятствиями для эффективного гражданского контроля. Важным фактором является также и отсутствие общественного доверия к антикоррупционным инициативам из-за низкой прозрачности деятельности государственных органов и частых случаев безнаказанности.

### **Перспективы и рекомендации.**

Для повышения эффективности борьбы с коррупцией в Казахстане необходимо усиливать роль гражданского общества и обеспечивать реальные механизмы

взаимодействия между общественными организациями и государственными структурами. Важным шагом является улучшение законодательства в области защиты прав и свобод активистов, создание благоприятных условий для деятельности НКО и обеспечение свободного доступа к информации о государственной деятельности.

Необходимо также усиливать образовательные программы, направленные на повышение антикоррупционной осведомленности среди граждан. Это позволит не только улучшить мониторинг, но и повысить культурный уровень восприятия коррупции как неприемлемого явления в обществе.

**Заключение.** В Казахстане роль гражданского общества в противодействии коррупции приобретает все большее значение. Институты гражданского общества, такие как НКО, СМИ, обычные граждане, играют важную роль в мониторинге государственных процессов, выявлении коррупционных схем и повышении прозрачности власти.

Однако для того, чтобы взаимодействие между государственными органами и гражданским обществом было эффективным, необходимо устранить ряд проблем, таких как недостаточная защита прав граждан, слабая правовая поддержка и отсутствие полноценного доступа к информации. Развитие этих механизмов и поддержка гражданского контроля, имеют важное значение для борьбы с коррупцией.

#### Список литературы:

1. Ким, Л. И. Общественные организации и антикоррупционная политика в Казахстане. Журнал общественных наук, 2018, [с. 34-45].
2. Transparency International. Corruption Perceptions Index 2020. Berlin
3. Указ Президента Республики Казахстан от 20 февраля 2021 года № 515. «О некоторых вопросах Агентства Республики Казахстан по финансовому мониторингу»
4. Касымова, М. С. Гражданское общество в Казахстане: перспективы и вызовы. Алматы: Наука, 2020.
5. Ким, Л. И. Общественные организации и антикоррупционная политика в Казахстане. Журнал общественных наук, 2018, [с. 34-45].
6. Тишков, В. А. Государственная и общественная борьба с коррупцией в постсоветских странах. Москва: РГГУ, 2017.
7. OECD. Public Governance and Anti-Corruption in Kazakhstan: Review of the Public Sector. Paris: OECD Publishing, 2020.
8. Молдабекова, Д. К. Роль институтов гражданского общества в антикоррупционной политике Казахстана. Астана: Издательство Академии государственного управления, 2019.
9. Кудряшова, А. В. Кризис доверия к государству и роль гражданского общества в противодействии коррупции. Журнал политических исследований, 2020, [с. 50-63].

UDC 347.1

Yergazy Aitzhan Muslimuly

Master's student  
in the Project Management program  
Astana IT University  
(Astana, Kazakhstan)

## METHODOLOGICAL MODEL FOR INTEGRATING AI TOOLS INTO BUSINESS PROCESSES BASED ON THE AGILE APPROACH

**Abstract:** The rapid integration of artificial intelligence (AI) into business environments has transformed traditional business process management (BPM) paradigms. However, the implementation of AI initiatives frequently encounters methodological challenges due to uncertainty, dynamic data environments, and organizational resistance. This study develops a methodological model for integrating AI tools into business processes based on the Agile approach. Using a systematic literature review, comparative analysis of project management methodologies (Waterfall vs Agile), synthesis of AI implementation frameworks, and conceptual modeling, the paper identifies structural limitations of traditional digitalization strategies and proposes an integrated AI–Agile methodological framework. The findings demonstrate that AI projects require iterative validation, hypothesis-driven experimentation, and flexible governance structures. The proposed model enhances adaptability, reduces implementation risks, and supports sustainable digital transformation in enterprises.

**Keywords:** Artificial Intelligence, Agile, Scrum, Business Process Management, Digital Transformation, Methodological Model

**Introduction.** Artificial intelligence (AI) has become a central enabler of contemporary digital transformation strategies across industries. AI-powered analytics, reinforcement learning, natural language processing, and predictive modeling increasingly shape enterprise decision-making, operational efficiency, risk assessment, and customer experience management [1; 13; 41]. Organizations are moving beyond simple automation toward intelligent process optimization, hyperautomation, and data-driven governance [8; 11]. According to global industry reports, AI adoption continues to accelerate; however, a significant proportion of AI initiatives fail to generate sustainable business value or scale beyond pilot phases [14; 15].

The paradox of rapid AI diffusion combined with high implementation failure rates suggests that technological maturity alone does not guarantee organizational success. While substantial progress has been achieved in deep learning architectures [9; 31], transformer-based language models [5; 39], and reinforcement learning systems capable of complex decision-making [16; 30], the managerial and methodological dimensions of AI integration remain comparatively underdeveloped.

AI projects differ fundamentally from traditional IT system deployments. They are characterized by:

- high data dependency and variability;
- probabilistic outputs rather than deterministic logic;
- iterative experimentation and model retraining;

- evolving performance metrics;
- regulatory, ethical, and explainability constraints [25; 19].

These characteristics introduce structural uncertainty that challenges conventional project management approaches.

Historically, many organizations have implemented digital technologies using sequential project methodologies such as Waterfall. While effective for stable and well-defined software engineering environments, linear methodologies assume that requirements can be specified in advance and that system outputs are predictable. Such assumptions conflict with the experimental and hypothesis-driven nature of AI development. Reinforcement learning models, predictive analytics systems, and natural language processing solutions require iterative validation cycles, frequent recalibration, and progressive business value assessment [6; 4].

Simultaneously, research on digital transformation increasingly highlights the importance of governance structures, change management mechanisms, and responsible AI frameworks [24; 34]. AI implementation is not purely a technical initiative but an organizational transformation process affecting workflows, roles, decision hierarchies, and risk management structures. Consequently, methodological alignment between AI development lifecycles and enterprise process management becomes critical.

Agile methodologies, including Scrum and Kanban, have emerged as flexible governance mechanisms suitable for environments characterized by uncertainty and rapid feedback cycles. Agile emphasizes iterative development, stakeholder collaboration, adaptive planning, and continuous improvement. Recent studies indicate that combining Agile principles with AI project management improves project adaptability, human–AI collaboration, and sustainability outcomes [35]. Furthermore, integrating data science process models such as CRISP-DM with Agile practices enhances coordination between technical experimentation and business objectives [7; 38].

Despite growing recognition of Agile's compatibility with AI development, the literature lacks a consolidated methodological framework that systematically integrates AI lifecycle management, business process analysis, and Agile governance principles into a unified model. Existing research tends to focus either on technical AI algorithms or on general digital transformation strategies without providing structured implementation pathways.

Therefore, a theoretical and methodological gap persists at the intersection of:

- AI technological development,
- business process management (BPM),
- and Agile project governance.

This study addresses that gap by proposing a conceptual methodological model for integrating AI tools into business processes based on Agile principles. The research adopts a desktop research methodology, including systematic literature review, comparative analysis of project management methodologies (Waterfall versus Agile), synthesis of AI implementation frameworks, and conceptual modeling.

The primary objective of this paper is to develop and justify an integrated AI–Agile methodological model that aligns AI experimentation cycles with structured business process transformation mechanisms. The study contributes to digital transformation theory by formalizing AI integration as a governance-driven, iterative, and value-oriented process rather than a purely technological deployment.

## Literature Review

### *Artificial Intelligence in Business Process Management*

Artificial intelligence has increasingly become embedded within business process management (BPM), transforming how organizations design, monitor, and optimize their operational workflows. Traditional BPM focused primarily on rule-based automation and process standardization; however, the integration of AI introduces predictive, adaptive, and autonomous capabilities that fundamentally redefine process governance.

Recent studies demonstrate that AI-driven predictive monitoring significantly enhances process visibility and anticipatory decision-making [4]. Reinforcement learning and machine learning techniques allow organizations to forecast bottlenecks, detect anomalies, and optimize operational performance in real time. Similarly, AI-powered decision support systems improve enterprise-level strategic alignment by integrating large-scale data analytics into managerial processes [12; 13].

Beyond operational optimization, AI applications extend to financial risk management [3], sustainability-oriented performance management [17], financial reporting quality enhancement [18], and customer interaction intelligence [41]. Machine learning models increasingly enable dynamic workflow adaptation and process intelligence, shifting BPM from static process mapping to continuously learning systems [36].

However, despite these advances, AI integration introduces structural and managerial complexities that differentiate it from conventional enterprise software systems. First, AI systems depend heavily on data quality and availability. Variability in datasets, bias, incompleteness, and evolving data distributions significantly influence model performance. Second, AI models—particularly deep learning architectures—often function as probabilistic systems, producing outputs with uncertainty rather than deterministic outcomes.

Model interpretability presents an additional challenge. High-performing black-box models may achieve predictive accuracy while remaining difficult to explain, raising accountability concerns in high-stakes business decisions [25]. Research on explainable AI [19] highlights the importance of transparency in predictive business process monitoring. Furthermore, AI adoption raises ethical, confidentiality, and regulatory issues, especially in jurisdictions where legal frameworks for AI governance remain under development [34].

Another defining feature of AI systems is the necessity for continuous retraining and performance recalibration. Unlike traditional IT systems that maintain stable functionality after deployment, AI models degrade if not updated in response to data drift or environmental changes. This dynamic nature requires ongoing monitoring and adaptation mechanisms embedded within organizational processes.

Taken together, these characteristics illustrate that AI projects are not merely technical deployments but dynamic learning systems integrated into business operations. As a result, conventional project management approaches may not sufficiently accommodate the uncertainty and iterative experimentation inherent in AI-based BPM.

### *Limitations of the Traditional Waterfall Methodology*

The Waterfall methodology has historically dominated software development and enterprise IT implementation. Its sequential structure—requirements definition, system design, development, testing, and deployment—provides clarity, documentation discipline, and control mechanisms. For projects with stable requirements and well-defined outputs, this linear model remains effective.

However, AI development fundamentally challenges the assumptions underlying Waterfall. AI systems rarely operate within environments where requirements can be fully specified at the outset. Instead, AI solutions evolve through experimentation, hypothesis testing, and performance iteration. Reinforcement learning systems, for example, improve via trial-and-error interactions with data environments [30]. Predictive models frequently require multiple cycles of feature engineering, validation, parameter optimization, and retraining [6].

Because model performance cannot be guaranteed in advance, fixed upfront specifications are often unrealistic. In AI projects, understanding of data limitations, model feasibility, and business value emerges progressively during experimentation. Consequently, rigid phase-gate structures delay feedback loops and increase the cost of late-stage adjustments.

A major risk associated with Waterfall in AI contexts is delayed validation. In linear methodologies, performance assessment typically occurs in the testing or deployment stages. If an AI model fails to meet expected accuracy or fails to deliver measurable business value, failure may only become apparent after substantial resource investment. This increases financial risk and organizational resistance.

Furthermore, AI solutions require post-deployment monitoring and iterative recalibration, activities not naturally embedded within the Waterfall structure. Therefore, while Waterfall ensures procedural control, it lacks the adaptive mechanisms necessary for managing uncertainty-driven AI development.

#### *Agile as a Response to AI-Induced Uncertainty*

Agile methodologies emerged as a response to dynamic and complex development environments. Unlike Waterfall, Agile frameworks such as Scrum and Kanban emphasize iterative cycles, incremental value delivery, continuous stakeholder feedback, and adaptive planning.

In AI contexts, these principles align closely with the experimental nature of model development. AI solutions are hypothesis-driven: teams formulate assumptions about data relationships, test models, evaluate performance, and iteratively refine approaches. Agile sprint cycles enable short development intervals during which models can be trained, evaluated, and adjusted based on measurable metrics.

Scrum provides structured roles, sprint planning sessions, backlog prioritization, and retrospective analysis, facilitating transparent collaboration between data scientists, developers, and business stakeholders. Kanban enhances workflow visibility and resource allocation efficiency, particularly in data pipeline management.

Empirical research suggests that integrating Agile principles into AI initiatives enhances project adaptability and cross-functional collaboration. Human–AI collaboration supported by Agile governance improves AI project success rates and sustainability outcomes [35]. Similarly, integrating CRISP-DM—a standard data mining lifecycle model—with Agile practices improves coordination between technical experimentation and business objectives [7; 38].

Agile frameworks reduce implementation risk by enabling early validation of business value, incremental deployment, and rapid course correction. Rather than committing to large-scale system rollouts, organizations can pilot AI models in controlled iterations, measure key performance indicators, and scale solutions progressively.

Moreover, Agile governance structures inherently support continuous monitoring and improvement, which aligns with the retraining and recalibration needs of AI systems. This structural compatibility suggests that Agile methodologies may provide a more appropriate

foundation for AI integration into business processes than traditional sequential models.

**Research Methodology.** This study adopts a qualitative desktop research design aimed at developing a conceptual methodological framework for integrating artificial intelligence (AI) into business processes using Agile principles. Desktop research is appropriate for theoretical model development where the objective is synthesis, comparison, and conceptual integration rather than empirical testing.

The methodological approach consists of four interrelated stages: systematic literature review, comparative methodological analysis, synthesis of AI lifecycle frameworks, and conceptual modeling.

#### *Systematic Literature Review*

The first stage involved a structured review of peer-reviewed academic publications addressing artificial intelligence integration, business process management (BPM), digital transformation, and project management methodologies. Sources were selected from journals indexed in major academic databases and included both foundational theoretical works and recent applied research.

The review focused on four thematic clusters:

- AI applications in business environments
- AI lifecycle and data science process models
- Project management methodologies (Waterfall, Agile, Scrum, Kanban)
- Governance, explainability, and responsible AI

The purpose of this stage was to identify recurring patterns, structural limitations, and methodological gaps within existing research. Particular attention was paid to studies analyzing predictive analytics implementation [27], AI-enabled BPM [36], and AI governance frameworks [24].

Rather than conducting a meta-analysis of quantitative findings, this review emphasizes conceptual convergence and theoretical positioning across disciplines.

#### *Comparative Analysis of Project Management Methodologies*

The second stage consisted of a comparative analytical evaluation of traditional Waterfall methodology and Agile frameworks in the context of AI implementation.

The comparison was structured along the following dimensions:

1. requirement stability
2. feedback cycle length
3. risk distribution
4. validation timing
5. adaptability to uncertainty
6. post-deployment monitoring capacity

Waterfall was analyzed as a sequential, phase-based model emphasizing upfront requirement definition and controlled progression. Agile methodologies (Scrum and Kanban) were examined as iterative governance structures enabling incremental delivery and continuous adaptation.

The analytical objective was not to evaluate general project management effectiveness, but to assess structural compatibility between methodological logic and AI system characteristics, such as probabilistic outputs, iterative model training, and evolving performance metrics.

#### *Synthesis of AI Lifecycle Frameworks*

The third stage involved synthesizing existing AI and data science lifecycle models to

identify their compatibility with business process transformation mechanisms.

Key frameworks examined include CRISP-DM as a structured data mining lifecycle [38], hyper automation models integrating AI, machine learning, and robotic process automation [8; 11], digital twin architectures for real-time operational monitoring [21; 22; 32], predictive analytics deployment models [27], and explainable AI mechanisms such as Grad-CAM [28].

This stage aimed to determine how AI technical lifecycles interact with enterprise governance structures. The analysis revealed that while AI lifecycle frameworks provide technical guidance for model development, they do not sufficiently address organizational alignment, iterative business validation, or project governance integration.

### *Conceptual Modeling*

The final stage consisted of developing a conceptual AI–Agile integration model based on insights derived from the previous stages.

Conceptual modeling was conducted through abstraction and structural integration of:

- AI development cycles
- BPM diagnostic stages
- Agile sprint mechanisms
- KPI-based validation systems
- Responsible AI governance principles

The objective was to design a unified methodological structure capable of aligning AI experimentation processes with enterprise transformation logic.

This modeling process is normative and prescriptive rather than descriptive. It proposes a structured implementation pathway grounded in theoretical synthesis and comparative analysis.

### *Research Validity and Scope*

As a desktop research study, this paper does not include empirical data collection or case-based statistical validation. Instead, its contribution lies in theoretical integration and methodological structuring.

The validity of the proposed framework is grounded in:

- convergence of findings across multiple peer-reviewed sources;
- cross-disciplinary synthesis between AI research and project management theory;
- logical alignment between AI system characteristics and Agile governance principles.

Future research may empirically validate the model through multi-case studies or longitudinal implementation analysis.

**Development of the AI–Agile Methodological Model.** Based on the synthesis of literature on artificial intelligence lifecycle management, business process management (BPM), and Agile governance structures, this study proposes a seven-stage AI–Agile methodological model. The purpose of this framework is to structurally align AI experimentation processes with enterprise transformation mechanisms in order to reduce implementation uncertainty and enhance measurable business value. The model integrates three conceptual domains: business process diagnostics, AI development lifecycle management, and Agile project governance. Unlike traditional digital transformation approaches that focus primarily on technological deployment, the proposed structure embeds AI integration within iterative validation cycles and structured performance control mechanisms.

The **first stage** of the model consists of an AS-IS business process diagnosis. Effective AI implementation requires a clear understanding of existing operational workflows. Without prior

process transparency, organizations risk automating inefficiencies rather than achieving meaningful optimization. Using BPM techniques and process mining approaches [33], enterprises can identify bottlenecks, redundant decision nodes, resource misallocations, and structural performance gaps. This stage establishes baseline metrics, including cycle time, error frequency, operational cost, and process variability. The purpose of the diagnostic phase is not technological selection but structural understanding, ensuring that AI solutions are grounded in operational realities.

The **second stage** involves AI potential identification. Not every business process benefits equally from AI integration, and therefore candidate use cases must be carefully evaluated. This model recommends assessing potential AI initiatives through a structured value–complexity analysis that considers expected business impact, data availability and reliability, technical feasibility, regulatory sensitivity, and organizational readiness. By systematically prioritizing high-impact yet feasible use cases, organizations avoid investing resources in low-value experimentation and reduce the risk of trend-driven technological adoption disconnected from strategic objectives.

The **third stage** formalizes AI integration as a hypothesis-driven process. AI systems are inherently experimental, as model performance cannot be guaranteed in advance. For this reason, each prioritized use case should be translated into measurable performance hypotheses. These hypotheses may relate to reductions in process cycle time, improvements in predictive accuracy, anomaly detection speed, cost reduction, or operational efficiency gains. Hypothesis formulation transforms AI implementation from exploratory experimentation into structured business validation. Clear success criteria enable early performance assessment and prevent ambiguity in evaluating project outcomes.

The **fourth stage** introduces AI backlog formation. Drawing from CRISP-DM principles [38], this stage organizes tasks related to business understanding, data preparation, modeling, evaluation, and deployment. However, unlike traditional CRISP-DM implementation, tasks are decomposed into incremental units compatible with Agile sprint cycles. This transformation ensures that data science activities are not isolated technical exercises but are integrated into structured governance mechanisms. The AI backlog functions as a dynamic coordination tool connecting technical experimentation with business value objectives.

The **fifth stage** centers on iterative sprint implementation, which represents the operational core of the AI–Agile framework. Short development cycles enable incremental model training, evaluation, and refinement. During each sprint, data pipelines are improved, model parameters are optimized, validation metrics are reviewed, and business stakeholders assess interim results. This iterative validation process reduces the likelihood of large-scale failure by enabling early course correction. If model performance does not satisfy predefined hypotheses, adjustments can be made without extensive sunk costs. This approach reflects the experimental nature of reinforcement learning and predictive analytics systems, ensuring structural compatibility between methodological governance and AI system behavior.

The **sixth stage** focuses on KPI-based evaluation. Unlike purely technical validation, this phase emphasizes measurable business impact. AI initiatives are assessed against predefined key performance indicators aligned with strategic objectives. Industry research indicates that AI projects succeed when directly linked to quantifiable business metrics rather than abstract innovation goals [14]. By embedding KPI evaluation within each sprint cycle, the model ensures continuous alignment between technological experimentation and enterprise value creation.

The **final stage** addresses scaling and governance. Once pilot implementations demonstrate validated performance improvements, AI solutions are integrated into enterprise architecture and operational decision systems. However, scaling requires structured governance mechanisms to ensure sustainability and regulatory compliance. Responsible AI principles—including model transparency, explainability, ethical data management, and risk monitoring—must be embedded within enterprise governance structures [25; 24]. Unlike static deployment models, this stage incorporates continuous monitoring and retraining protocols to address data drift and environmental variability.

Collectively, the AI–Agile methodological model bridges the gap between technical AI lifecycle experimentation and structured business transformation governance. By integrating BPM diagnostics, hypothesis-driven AI experimentation, iterative Agile control mechanisms, KPI-based validation, and responsible governance principles, the model provides a coherent and scalable pathway for AI integration. It reframes AI implementation not as a one-time technological deployment but as an adaptive, value-oriented, and continuously evolving organizational capability.

**Discussion.** The proposed AI–Agile methodological model contributes to the evolving discourse on digital transformation by addressing several structural gaps identified in the literature. While existing research has extensively explored AI technologies, predictive analytics, reinforcement learning systems, and process intelligence mechanisms, comparatively limited attention has been devoted to the governance structures required for their sustainable integration into business environments. This study argues that the success of AI initiatives depends not solely on algorithmic sophistication, but on methodological alignment between technological experimentation and organizational management frameworks.

One of the primary contributions of the model lies in aligning AI lifecycle experimentation with Agile governance principles. AI systems are inherently probabilistic and iterative. Their development requires repeated cycles of model training, evaluation, recalibration, and validation. Traditional project governance structures, particularly sequential phase-gate methodologies, are not designed to accommodate such dynamic experimentation. By embedding AI development into sprint-based governance cycles, the proposed framework structurally integrates uncertainty management into the project lifecycle. This alignment reduces rigidity and enables progressive value realization rather than delayed performance assessment.

The model also incorporates explainability and responsible AI principles into the scaling phase of implementation. Contemporary literature emphasizes that AI adoption must address transparency, accountability, and regulatory compliance challenges [25; 24]. High-performing models that lack interpretability can undermine organizational trust and expose enterprises to legal and reputational risks. By integrating responsible AI governance into the methodological structure rather than treating it as an afterthought, the framework promotes sustainable transformation. Ethical data management, performance monitoring, and explainability mechanisms become embedded components of enterprise architecture rather than reactive compliance measures.

Another significant contribution concerns sustainability and regulatory adaptability. AI-driven business process transformation operates within complex regulatory environments, particularly in emerging markets where legal frameworks for AI governance continue to evolve [34]. The iterative nature of the AI–Agile model allows organizations to adapt incrementally to regulatory updates and stakeholder expectations. This adaptive capacity enhances long-term

viability and reduces systemic risk.

Furthermore, the model mitigates late-stage implementation failures, a common problem in large-scale AI initiatives. Industry analyses indicate that many AI projects fail not due to technical limitations, but due to insufficient integration with business processes and unclear value metrics [14]. By formalizing hypothesis-driven experimentation and embedding KPI-based validation into each sprint cycle, the framework ensures continuous performance assessment. This reduces the likelihood of large-scale resource expenditure on non-viable models and supports early-stage course correction.

Unlike traditional digitalization strategies, which often prioritize technology acquisition or infrastructure modernization, the AI–Agile framework prioritizes measurable business value and iterative organizational learning. Digital transformation frequently emphasizes system implementation milestones rather than sustained performance improvement. In contrast, the proposed model reframes AI adoption as a dynamic learning system, where organizational capabilities evolve alongside technological refinement. This shift from technology-centric transformation to value-centric transformation represents a critical theoretical advancement.

The integration of CRISP-DM principles with Agile governance further strengthens the model's structural coherence [38]. CRISP-DM provides a robust lifecycle structure for data mining and analytics projects, yet it does not inherently define project governance mechanisms or iterative sprint coordination. By embedding CRISP-DM cycles into an Agile backlog environment, the model bridges the gap between data science workflows and enterprise-level management structures. This integration ensures that technical experimentation remains aligned with strategic objectives and resource allocation constraints.

From a theoretical perspective, the framework contributes to digital transformation research by conceptualizing AI implementation as a multi-layered governance process rather than a technological upgrade. It integrates insights from business process management, data science lifecycle theory, and Agile project governance into a unified methodological structure. This interdisciplinary synthesis addresses fragmentation in existing literature, where AI research often remains technically focused while management research lacks structured AI lifecycle integration.

Nevertheless, the model remains conceptual and requires empirical validation across diverse industries and organizational contexts. Future research should examine its practical applicability through longitudinal case studies, multi-industry comparisons, and quantitative impact assessment. Such empirical testing would further refine the model and strengthen its generalizability.

Overall, the AI–Agile methodological framework advances understanding of how organizations can systematically manage uncertainty, reduce implementation risk, and achieve sustainable AI-driven business transformation. It shifts the discourse from algorithmic capability toward governance alignment, thereby contributing to both theoretical development and practical implementation strategy.

**Conclusions.** This study demonstrates that artificial intelligence implementation differs fundamentally from traditional IT project deployment due to its inherent uncertainty, data dependency, and iterative experimentation requirements. Unlike deterministic software systems, AI solutions operate within probabilistic environments where performance evolves through continuous model training, validation, and recalibration. These structural characteristics necessitate governance mechanisms capable of accommodating experimentation, adaptive learning, and ongoing performance evaluation.

The analysis confirms that the traditional Waterfall methodology is structurally limited in AI contexts. Its sequential logic assumes stable requirements and delayed validation, conditions that are incompatible with the dynamic and exploratory nature of AI model development. In contrast, Agile approaches provide governance structures that better accommodate evolving performance metrics, iterative hypothesis testing, and incremental value realization. By enabling short development cycles, stakeholder feedback integration, and adaptive backlog management, Agile methodologies align more closely with the operational logic of AI systems.

Furthermore, the study emphasizes that successful AI integration requires structured hypothesis validation rather than exploratory experimentation without predefined performance criteria. Formalizing measurable hypotheses ensures that AI initiatives remain aligned with strategic objectives and quantifiable business value. This transformation from technology-driven experimentation to value-oriented validation reduces implementation ambiguity and enhances accountability.

The proposed hybrid AI–Agile methodological model enhances organizational adaptability and mitigates implementation risk by embedding AI lifecycle experimentation within structured governance mechanisms. By integrating AS-IS process diagnostics, value-based prioritization, iterative sprint development, KPI-driven evaluation, and responsible AI governance, the framework provides a coherent pathway for sustainable transformation. It bridges the gap between business process management, data science lifecycle structures such as CRISP-DM, and Agile project governance, creating a scalable and integrative implementation architecture.

From a theoretical perspective, the model contributes to digital transformation research by conceptualizing AI implementation as a governance-aligned organizational capability rather than a one-time technological upgrade. It reframes AI integration as an iterative learning system embedded within enterprise processes and controlled through structured validation mechanisms. This interdisciplinary synthesis advances the discourse at the intersection of artificial intelligence, business process management, and project governance theory.

Despite its conceptual contribution, this study is limited by its desktop research design and absence of empirical validation. Future research should test the applicability and effectiveness of the AI–Agile framework across multiple industries, organizational sizes, and regulatory environments. Longitudinal case studies and quantitative impact assessments would further refine the model and enhance its generalizability.

In conclusion, the AI–Agile methodological framework provides a structured, adaptable, and governance-oriented approach to integrating artificial intelligence into business processes. By aligning technological experimentation with organizational control mechanisms, it increases the likelihood of sustainable value realization and reduces systemic implementation risk in AI-driven digital transformation initiatives.

### References:

1. Agu A. T., Chukwu C. O. The integration of artificial intelligence (AI) into business processes // Journal of Digital Transformation Studies. 2023. URL: <https://www.researchgate.net/publication/375489528>
2. Ahmed H. M., El-Sherif N. The impact of artificial intelligence on the assessment of business reputation of enterprises // Journal of Business Reputation Studies. 2024. Vol. 8, № 4. P. 202–220. URL: <https://www.researchgate.net/publication/398263338>

3. Aziz M. J., Nur B. Artificial intelligence in financial risk management: Global trends, XAI, and regulatory approaches in Kazakhstan // *Central Asian Journal of Finance & AI*. 2023. Vol. 5, № 2. P. 99–118. URL: <https://www.researchgate.net/publication/398976250>
4. Bousdekis A., Apostolou D., Mentzas G. Modelling and predictive monitoring of business processes using reinforcement learning // *Sensors*. 2023. Vol. 23, № 15. Art. 6931. DOI: 10.3390/s23156931
5. Devlin J., Chang M.-W., Lee K., Toutanova K. BERT: Pre-training of deep bidirectional transformers for language understanding // *Proceedings of NAACL-HLT*. 2019.
6. García J., Fernández F. A comprehensive survey on safe reinforcement learning // *Journal of Machine Learning Research*. 2015. Vol. 16, № 1. P. 1437–1480.
7. García L., Fernandez M., Ruiz D. Integrating CRISP-DM and eXtreme programming in agile data science projects // *European Journal of Electrical Engineering and Computer Science*. 2024. Vol. 8, № 2. P. 45–58.
8. Haleem A., Javaid M., Singh R. P. Hyperautomation for the enhancement of automation in business processes // *Materials Today: Proceedings*. 2021. Vol. 45. P. 4171–4176. DOI: 10.1016/j.matpr.2021.02.658
9. He K., Zhang X., Ren S., Sun J. Deep residual learning for image recognition // *Proceedings of CVPR*. 2016. P. 770–778.
10. Hernandez L. M., Zhao Q. Integrating artificial intelligence into business // *Global Journal of Information Systems*. 2024.
11. Jangam S. Hyperautomation: A combination of AI, ML, and robotic process automation for Industry 5.0 // *International Journal of AI & Data Science in Machine Learning*. 2024. Vol. 3, № 1. P. 22–34.
12. Kim J. H., Torres L. Integrating artificial intelligence (AI) and business intelligence (BI): A framework for improving enterprise performance // *Journal of Enterprise Performance Optimization*. 2023. Vol. 9, № 3. P. 122–139.
13. Lee S. Y., Gupta A. Optimizing decision-making in digital business processes through artificial intelligence // *Journal of AI in Business Analytics*. 2024. Vol. 5, № 1. P. 15–29.
14. McKinsey & Company. The future of predictive operations: Using data and analytics to build resilient organizations. McKinsey Global Institute, 2021.
15. McKinsey & Company. The state of AI in 2021. McKinsey Global Institute, 2021. URL: <https://www.mckinsey.com>
16. Mnih V. et al. Human-level control through deep reinforcement learning // *Nature*. 2015. Vol. 518, № 7540. P. 529–533.
17. Nwokoro A. M., Eze F. O. Artificial intelligence (AI) integration and business sustainability in Enugu State // *Nigerian Journal of Sustainable Business*. 2023. Vol. 7, № 3. P. 54–71.
18. Okoye U. C., Mensah K. Influence of artificial intelligence integration on financial reporting quality // *Journal of Financial Analytics & AI*. 2023. Vol. 10, № 2. P. 89–107.
19. Ouyang C., Sindhgatta R., Moreira C. Explainable AI enabled inspection of business process prediction models // *arXiv*. 2021. URL: <https://arxiv.org/abs/2107.09767>
20. Patel D. R., Singh T. Integration of artificial intelligence into business processes // *International Journal of Enterprise Science*. 2023.

21. Qi Q., Tao F. Digital twin and big data towards smart manufacturing and Industry 4.0 // IEEE Access. 2018. Vol. 6. P. 3585–3593.
22. Rasheed A., San O., Kvamsdal T. Digital twin: Values, challenges, and enablers from a modeling perspective // IEEE Access. 2020. Vol. 8. P. 21980–22012.
23. Reddy P., Banerjee S. Artificial intelligence in business intelligence: AI-powered BI // Journal of Intelligent Data Systems. 2024. Vol. 12, № 1. P. 44–61.
24. Roberts K. L., Huang X. Artificial intelligence and business process management: A responsible framework // Journal of Sustainable Digital Transformation. 2024. Vol. 6, № 1. P. 88–104.
25. Rudin C. Stop explaining black box machine learning models for high-stakes decisions // Nature Machine Intelligence. 2019. Vol. 1, № 5. P. 206–215. DOI: 10.1038/s42256-019-0048-x
26. Rzepka R., Mirończuk M., Włodarczyk P. Conversational AI in customer service // Journal of Intelligent Information Systems. 2022. Vol. 59, № 3. P. 553–575.
27. SAS Institute. Predictive analytics: Concepts, algorithms, and business applications. 2023.
28. Selvaraju R. R. et al. Grad-CAM: Visual explanations from deep networks // Proceedings of ICCV. 2017. P. 618–626.
29. Smith R. J., Kumar P. Integration of AI technologies into business processes // International Journal of AI & Business Research. 2024.
30. Sutton R. S., Barto A. G. Reinforcement learning: An introduction. 2nd ed. Cambridge: MIT Press, 2018.
31. Szegedy C. et al. Rethinking the inception architecture for computer vision // Proceedings of CVPR. 2016. P. 2818–2826.
32. Tao F. et al. Digital twin-driven product design, manufacturing, and service with big data // International Journal of Advanced Manufacturing Technology. 2019. Vol. 94. P. 3563–3576.
33. Tax N., Sidorova N., van der Aalst W. M. P. Discovering structured workflows from natural language texts // Information Systems. 2020. Vol. 93. Art. 101563. DOI: 10.1016/j.is.2020.101563
34. Tulegenova A., Ismailov D. Confidentiality and trust in AI-assisted mediation // Eurasian Journal of Digital Law & AI. 2023. Vol. 2, № 3. P. 77–94.
35. Walker S. P., Choi E. Generative AI and human-AI collaboration // International Journal of Agile Digital Transformation. 2024. Vol. 1, № 1. P. 1–22.
36. Weinzierl S., Zilker S., Dunzer S. Machine learning in business process management // Expert Systems with Applications. 2024. Vol. 253. Art. 124181. DOI: 10.1016/j.eswa.2024.124181
37. Wickramanayake B., Moreira C., Ouyang C. Building interpretable models for business process predictions // arXiv. 2021.
38. Wirth R., Hipp J. CRISP-DM: Towards a standard process model for data mining // Proceedings of the 4th International Conference on Knowledge Discovery and Data Mining. 2000. P. 29–39.
39. Xu Y. et al. LayoutLM: Pre-training of text and layout for document image understanding // Proceedings of ACM SIGKDD. 2020. P. 1192–1200.

40. Zhang Z., Wang Y., Qiao Y. Real-time computer vision for industrial safety monitoring // IEEE Transactions on Industrial Informatics. 2021. Vol. 17, № 9. P. 6040–6052.
41. Zhao Y., Martinez R. Study of the role of artificial intelligence in retail business // Journal of Retail Analytics & AI. 2024. Vol. 3, № 4. P. 55–73.

УДК 658.5

**Темербаев Ержан Жуматаевич**генеральный директор  
ООО «TRADE-Инжиниринг»,  
(г.Павлодар, Казахстан)**МОДЕЛИ ОТВЕТСТВЕННОСТИ ЗА АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ В  
ПРОИЗВОДСТВЕННЫХ ОРГАНИЗАЦИЯХ**

**Аннотация:** Статья посвящена исследованию моделей юридической ответственности за вред, причинённый автоматизированными и автономными системами в производственных организациях. В работе рассматриваются технические основы функционирования автоматизированных систем управления, международные стандарты безопасности и функциональной надёжности, а также правовые механизмы возмещения вреда. Проанализированы национальные и зарубежные подходы к распределению ответственности между производителем оборудования, разработчиком программного обеспечения, интегратором и эксплуатирующей организацией. Особое внимание уделено риск-ориентированному регулированию, модернизации продуктовой ответственности в цифровой сфере и перспективным моделям распределения рисков. Выявлены проблемы правоприменения, связанные с установлением причинной связи, доказательственной асимметрией и обновляемым характером программного обеспечения. Сформулированы направления совершенствования правового регулирования с учётом технологической специфики автоматизированных систем.

**Ключевые слова:** автоматизированные системы, автономные системы, промышленная автоматизация, юридическая ответственность, распределение рисков, дефект продукции, программное обеспечение, риск-ориентированный подход, промышленная безопасность, страхование технологических рисков.

**Актуальность исследования.** В условиях цифровизации промышленности и широкого внедрения автоматизированных систем управления производственными процессами вопросы юридической ответственности за результаты их функционирования приобретают особую значимость. Производственные организации активно используют промышленные роботы, программно-аппаратные комплексы и интеллектуальные системы, что повышает эффективность производства, но одновременно создаёт новые правовые риски.

Эксплуатация автоматизированных систем связана с возможностью технических сбоев, программных ошибок и иных факторов, способных повлечь причинение вреда жизни и здоровью работников, имущественный ущерб и нарушение требований безопасности. При высокой степени автономности таких систем усложняется определение субъекта ответственности и разграничение обязанностей между производителем оборудования, разработчиком программного обеспечения и эксплуатирующей организацией.

Действующие нормы законодательства предусматривают ответственность за причинение вреда и за нарушение требований безопасности, однако специфика

современных автоматизированных комплексов требует уточнения механизмов распределения рисков. В связи с этим исследование моделей ответственности за автоматизированные системы в производственных организациях является актуальным и обусловлено необходимостью адаптации правового регулирования к условиям технологической модернизации.

**Цель исследования.** Целью данного исследования является комплексный анализ моделей юридической ответственности за вред, причинённый автоматизированными и автономными системами в производственных организациях, а также выявление перспективных направлений совершенствования механизмов распределения рисков с учётом технологической специфики современных цифровых решений.

**Материалы и методы исследования.** Материальную основу исследования составили нормы гражданского законодательства о возмещении вреда, международные стандарты безопасности и функциональной надёжности, официальные материалы, посвящённые регулированию систем искусственного интеллекта и автономных технологий, а также научные публикации по вопросам ответственности за цифровые продукты.

В работе использованы формально-юридический метод, системный анализ, сравнительно-правовой метод и метод правового моделирования.

**Результаты исследования.** Автоматизация производственных процессов представляет собой объективный этап развития промышленности, связанный с применением технических средств и программного обеспечения для выполнения функций управления, контроля и регулирования без непосредственного участия человека либо с его минимальным участием. В промышленной практике широко используются автоматизированные системы управления технологическими процессами, промышленные роботы и программируемые логические контроллеры. Их применение регламентируется техническими стандартами и требованиями безопасности, установленными в международных и национальных нормативных документах [1].

Согласно определению, закреплённому в международном стандарте ISO 8373, промышленный робот представляет собой автоматически управляемый, перепрограммируемый многофункциональный манипулятор с тремя и более осями, который может быть стационарным или мобильным и применяется в промышленной автоматизации (рисунок 1). Требования безопасности к роботам и робототехническим системам установлены стандартом ISO 10218, предусматривающим обязательность оценки рисков, защитных ограждений и средств аварийной остановки. В сфере автоматизированных систем управления технологическими процессами применяются стандарты серии IEC 61508, устанавливающие требования к функциональной безопасности электрических, электронных и программируемых электронных систем.



Рис. 1. Промышленный робот-манипулятор [4]

Юридическая ответственность в условиях автоматизации базируется на общеправовых категориях вины, причинной связи и вреда. В гражданском праве ответственность за причинение вреда строится на принципе полного возмещения ущерба при наличии противоправного поведения, вреда, причинной связи и вины, если законом не предусмотрена ответственность независимо от вины. В отношении деятельности, связанной с повышенной опасностью для окружающих, применяется режим ответственности владельца источника повышенной опасности, при котором обязанность возмещения вреда наступает независимо от вины при условии причинной связи между деятельностью и наступившими последствиями.

Особенность автоматизированных производственных систем заключается в сочетании материального объекта и программного алгоритма. Это обуславливает необходимость разграничения ответственности между изготовителем оборудования, разработчиком программного обеспечения и эксплуатирующей организацией. В правовой доктрине признаётся, что дефекты конструкции и производственные недостатки относятся к сфере ответственности изготовителя, тогда как нарушение правил эксплуатации либо несоблюдение требований безопасности влечёт ответственность эксплуатирующего субъекта. Если вред вызван программной ошибкой, оценка производится с учётом характера дефекта, соблюдения технических стандартов и наличия сертификации.

В целях обеспечения безопасности функционирования автоматизированных систем применяется риск-ориентированный подход, предусматривающий обязательную оценку и классификацию рисков. В стандарте ISO 12100 закреплены принципы идентификации опасностей, анализа и снижения риска при проектировании машин и оборудования. Процедура оценки включает определение возможного ущерба, вероятности его наступления и тяжести последствий.

В современных производственных организациях автоматизированные системы управления строятся по иерархическому принципу. Типовой пример такой архитектуры представлен на рисунке 2.

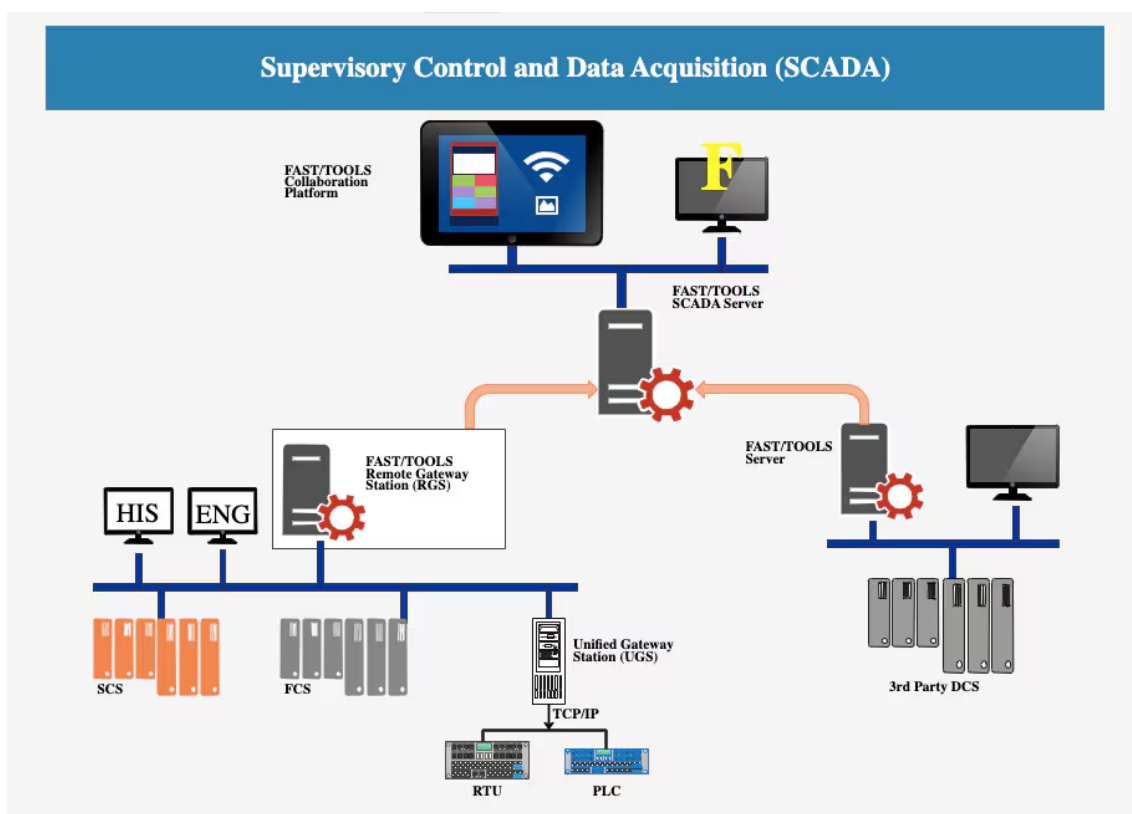


Рис. 2. Архитектура системы диспетчерского управления и сбора данных (SCADA) в производственной организации [5]

В национальных правовых системах ответственность за вред, причинённый автоматизированными производственными системами, формируется на основе сочетания нескольких правовых режимов: ответственности изготовителя за дефектный продукт, деликтной ответственности за причинение вреда и ответственности эксплуатирующей организации за нарушение требований безопасности. Конкретная квалификация зависит от источника дефекта и распределения контроля над риском.

Основные направления распределения ответственности представлены в таблице 1.

**Таблица 1 - Основные направления распределения ответственности**

| Сфера риска                                 | Потенциальный субъект ответственности | Правовая квалификация                                        |
|---------------------------------------------|---------------------------------------|--------------------------------------------------------------|
| Конструкторский или производственный дефект | Изготовитель                          | Ответственность за дефектный продукт                         |
| Ошибка программного обеспечения             | Разработчик / поставщик               | Дефект продукции или нарушение обязательств                  |
| Ненадлежащее внедрение и настройка          | Интегратор                            | Договорная и деликтная ответственность                       |
| Нарушение правил эксплуатации               | Эксплуатирующая организация           | Деликтная ответственность, нарушение требований безопасности |

*Источник: разработка автора.*

Зарубежные подходы к регулированию автономных систем строятся на сочетании риск-ориентированного регулирования, модернизированной продуктовой ответственности и требований к корпоративному управлению рисками. Регуляторы

стремятся не только обеспечить компенсацию вреда, но и заранее встроить механизмы предотвращения рисков, обязательной документации и контроля на протяжении жизненного цикла системы.

В европейской модели закреплён риск-ориентированный подход к регулированию систем искусственного интеллекта. Нормативная рамка предусматривает классификацию систем по уровням риска и установление дифференцированных требований, включая специальные обязанности для высокорисковых систем. Дополнительно модернизируется режим ответственности за дефектную продукцию с учётом цифровых компонентов и программного обеспечения. В публичных обзорах реформы подчёркивается расширение понятия продукта на программные элементы и учёт обновлений и кибербезопасности при оценке дефекта.

В Великобритании принят специальный закон об автоматизированных транспортных средствах, предусматривающий выделение уполномоченного субъекта, ответственного за безопасное функционирование системы в автономном режиме. В США значительную роль играет управленческий подход через добровольные стандарты и рамки управления рисками.

Основные зарубежные механизмы регулирования автономных систем описаны в таблице 2.

**Таблица 2 - Основные зарубежные механизмы регулирования автономных систем**

| Подход                                                               | Что регулируется                                               | Ключевой механизм подотчётности / ответственности                                                                                         |
|----------------------------------------------------------------------|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Риск-ориентированное регулирование ИИ                                | Требования к системам в зависимости от уровня риска + надзор   | Поэтапное применение обязанностей, отдельные требования к «высокорисковым» и к моделям общего назначения, институты управления и контроля |
| Модернизированная продуктовая ответственность для цифровых продуктов | Вред от дефектной продукции с учётом ПО / цифровых компонентов | Расширение охвата на ПО / цифровые элементы, акцент на обновлениях / кибербезопасности, инструменты облегчения доказывания                |
| «Назначение ответственного субъекта» для автономного режима          | Специальный режим для автономных транспортных средств          | Выделение уполномоченного субъекта, ответственного за безопасное функционирование при самоуправлении                                      |
| Добровольная управленческая рамка рисков ИИ                          | Практики управления рисками в организациях                     | Структура процессов управления рисками на жизненном цикле (ориентир для «надлежащей осмотрительности»)                                    |
| Руководства по корпоративной ответственности и практике применения   | Рекомендации для организаций по ответственному ИИ              | Описанные практики внутреннего управления и контроля + обновления под новые риски                                                         |

*Источник: разработка автора.*

Таким образом, зарубежные подходы характеризуются комплексностью: ответственность за автономные системы рассматривается не изолированно, а в сочетании с обязательствами по управлению рисками, кибербезопасности, документированию и надзору, что направлено на снижение вероятности причинения вреда и повышение прозрачности распределения ответственности.

Современные подходы к распределению ответственности за автономные и автоматизированные системы формируются по нескольким направлениям. Наиболее обсуждаемой является модель строгой ответственности оператора высокорисковой системы. Её суть заключается в возложении обязанности по возмещению вреда независимо от доказывания вины, если вред причинён в процессе эксплуатации автономной системы. Такая модель направлена на устранение сложностей доказывания в условиях технической сложности алгоритмов и повышенной автономности решений [3].

Второе направление связано с распределённой ответственностью участников жизненного цикла системы. В этом случае ответственность разграничивается между разработчиком программного обеспечения, производителем оборудования, интегратором и эксплуатирующей организацией. Подход основывается на оценке того, на каком этапе – проектирования, производства, внедрения или эксплуатации – возник дефект либо нарушение требований безопасности. Такая модель обеспечивает более точное распределение рисков и учитывает технологическую специфику автономных систем.

Третьим перспективным механизмом рассматривается страховая модель, предусматривающая обязательное страхование вреда, причинённого автономными системами. Страхование позволяет обеспечить гарантированное возмещение ущерба независимо от сложности установления виновного лица и снижает финансовые риски для участников оборота.

Отдельно следует отметить отказ от концепции самостоятельной «электронной правосубъектности» автономных систем. Современная правовая позиция ориентирована на сохранение ответственности за людьми и организациями, контролирующими разработку и эксплуатацию технологий, поскольку именно они принимают решения и извлекают экономическую выгоду.

Для систематизации изложенных подходов и наглядного сопоставления их ключевых характеристик целесообразно представить основные перспективные модели распределения ответственности в обобщённом виде (таблица 3).

**Таблица 3 - Перспективные модели распределения ответственности**

| Модель                            | Содержание                                                                                | Практическая цель                                  |
|-----------------------------------|-------------------------------------------------------------------------------------------|----------------------------------------------------|
| Строгая ответственность оператора | Возмещение вреда без доказывания вины при эксплуатации высокорисковой системы             | Упрощение защиты потерпевшего                      |
| Распределённая ответственность    | Разграничение обязанностей между разработчиком, производителем, интегратором и оператором | Справедливое распределение рисков                  |
| Страховая модель                  | Обязательное страхование вреда от автономных систем                                       | Гарантированное возмещение ущерба                  |
| Отказ от «электронной личности»   | Сохранение ответственности за людьми и организациями                                      | Предотвращение размывания субъекта ответственности |

*Источник: разработка автора.*

Практика применения норм об ответственности за вред, причинённый автоматизированными и автономными системами, выявляет ряд устойчивых проблем. Основная из них – установление причинной связи между функционированием алгоритма или технического компонента и наступившими последствиями. Высокая степень

автономности, использование сложных программных решений и возможность изменения поведения системы в процессе эксплуатации затрудняют реконструкцию механизма причинения вреда [2].

Существенной проблемой остаётся доказательственная асимметрия: техническая документация и данные о работе системы находятся у разработчика или эксплуатирующей организации, что осложняет защиту прав потерпевших. Кроме того, на практике возникают сложности при разграничении договорной и внедоговорной ответственности, особенно в случаях комплексного внедрения автоматизированных решений.

Дополнительные вопросы связаны с обновляемым характером программного обеспечения. Изменения алгоритмов и установка обновлений требуют определения, кто несёт ответственность за последствия – разработчик, поставщик или оператор системы.

Совершенствование законодательства предполагает уточнение понятий, связанных с автономностью и уровнем риска, закрепление обязанностей по документированию работы систем, а также формирование процессуальных механизмов, обеспечивающих баланс интересов сторон. Важным направлением остаётся согласование правовых норм с международными стандартами безопасности и управления рисками.

**Выводы.** Проведённое исследование показало, что традиционные модели гражданско-правовой ответственности требуют адаптации к условиям цифровизации промышленности. Специфика автономных и автоматизированных систем проявляется в распределённом характере их функционирования, сложности установления причинной связи и необходимости учёта программных компонентов и обновлений.

Перспективными направлениями развития правового регулирования являются сочетание строгой ответственности оператора высокорисковой системы, распределённой ответственности участников жизненного цикла технологии и механизмов страхового обеспечения вреда. Совершенствование законодательства должно быть ориентировано на уточнение понятийного аппарата, повышение прозрачности функционирования систем и обеспечение баланса интересов участников правоотношений в условиях технологической модернизации производства.

### Литература:

1. Автоматизация процессов производства: понятие, принципы, методы [Электронный ресурс]. – Режим доступа: <https://academy-of-capital.ru/blog/avtomatizatsiya-protssesov-proizvodstva/>.
2. Апостолова Н.Н. Ответственность за вред, причиненный искусственным интеллектом // Северо-Кавказский юридический вестник. – 2021. – № 1. – С. 112-119. – DOI 10.22394/2074-7306-2021-1-1-112-119.
3. Казанцев Д.А. Правовые механизмы распределения ответственности за вред, причиненный системами искусственного интеллекта // Journal of Digital Technologies and Law. – 2025 – № 3(3). – С.446-471. – <https://doi.org/10.21202/jdtl.2025.18>.
4. Промышленный робот YASKAWA MOTOMAN GP110 [Электронный ресурс]. – Режим доступа: <https://roboplus.ru/industrial-robots/gp110?ysclid=mlyzv482jk603845439>.
5. Dominando los Diagramas de Bloques de Sistemas SCADA [Электронный ресурс]. – Режим доступа: <https://edraw.wondershare.es/database-tips/block-diagram-of-scada-system.html>.

УДК 334.72

**Мустафин Куаныш**основатель,  
Green Moving LLC  
(Калифорния, США, Ирвайн)**СТАНДАРТИЗАЦИЯ И КОМПЛАЕНС В МУВИНГОВОЙ ИНДУСТРИИ США:  
ОПЕРАЦИОННАЯ МОДЕЛЬ МАСШТАБИРОВАНИЯ ЧЕРЕЗ ФРАНЧАЙЗИНГ**

**Аннотация:** Статья посвящена анализу роли стандартизации и комплаенса в мувинговой индустрии США и их значению для построения операционной модели, позволяющей эффективно масштабировать бизнес через франчайзинг. Рассматриваются ключевые нормативные требования, регулирующие деятельность мувинговых компаний, а также отраслевые стандарты качества, влияющие на безопасность, прозрачность и доверие клиентов. Особое внимание уделено тому, как формализация процессов, внедрение единых регламентов, контроль соблюдения процедур и системный подход к управлению рисками обеспечивают воспроизводимость бизнес-модели и позволяют франчайзи поддерживать единый уровень сервиса независимо от региона. В статье также анализируются механизмы адаптации корпоративных стандартов к специфике локальных рынков, роль цифровых инструментов мониторинга и аудита, а также значение обучения персонала и сертификации для поддержания операционной устойчивости. Делается вывод, что стандартизация и комплаенс являются ключевыми опорными элементами масштабируемых франчайзинговых систем, обеспечивая устойчивый рост, минимизацию операционных ошибок и укрепление бренда в высококонкурентной среде мувингового бизнеса США.

**Ключевые слова:** мувинговая индустрия США, стандартизация, комплаенс, франчайзинг, операционная модель, масштабирование, регламенты, контроль качества, нормативные требования, управление рисками, сервисные стандарты, логистика, корпоративные процедуры.

**Актуальность исследования.** Мувинговая индустрия США является одной из наиболее динамично развивающихся сфер логистического сервиса, характеризующейся высоким уровнем конкуренции, существенными регуляторными требованиями и растущими ожиданиями клиентов в части прозрачности, безопасности и стандарта обслуживания.

На фоне цифровизации, ужесточения контроля со стороны федеральных и штатных органов и увеличения числа франчайзинговых сетей возрастает потребность в выработке единых стандартов и системы комплаенса, которые обеспечивают воспроизводимость и предсказуемость бизнес-процессов.

Актуальность исследования обусловлена необходимостью понимания того, как стандартизация и комплаенс формируют операционную модель масштабирования через франчайзинг, а также каким образом данные механизмы позволяют снижать риски, укреплять бренд, обеспечивать единый уровень сервиса и поддерживать операционную эффективность на национальном уровне.

**Цель исследования.** Цель работы состоит в комплексном анализе роли стандартизации и комплаенса в построении операционной модели мувинговых компаний США, ориентированной на масштабирование через франчайзинг. Исследование направлено на выявление ключевых регуляторных требований, описание эффективных корпоративных стандартов, изучение методов контроля соблюдения процедур и определение того, как стандартизированные процессы способствуют устойчивому развитию франчайзинговых сетей в условиях конкурентного рынка.

**Материалы и методы исследования.** В исследовании использованы данные федеральных и штатных нормативных актов, регулирующих деятельность мувинговых компаний, включая требования Министерства транспорта США и Федерального управления по безопасности автотранспорта.

Привлечены корпоративные регламенты ведущих франчайзинговых сетей, отраслевые стандарты качества обслуживания, аналитические отчёты логистических ассоциаций и данные рыночных исследований.

Методологическая база включает сравнительный анализ корпоративных и регуляторных требований, структурно-функциональный подход к оценке операционных процессов, методы контент-анализа документации и кейс-анализ успешных франчайзинговых моделей. Такой комплекс методов позволил выявить взаимосвязь между уровнем стандартизации, качеством комплаенс-процессов и степенью масштабируемости бизнес-модели.

**Результаты исследования.** Формирование системных стандартов и норм комплаенса в мувинговой индустрии США началось в первой половине XX века, когда рост автомобильных перевозок потребовал единых правил контроля качества и безопасности.

Первые регуляторные рамки возникли с созданием Межштатной торговой комиссии (ICC), которая установила базовые требования к перевозчикам, тарифам, ответственности за груз и лицензированию. Эти нормы стали фундаментом для последующего структурирования отрасли.

С середины XX века развитие интенсивной миграции населения, увеличение количества частных грузоперевозчиков и распространение межштатного бизнеса привели к необходимости ужесточения контроля. Постепенно формировались стандарты процессов упаковки, транспортировки, страхования и документооборота. В этот период появляется практика унифицированных контрактов и обязательств перевозчика перед клиентом, что повышало прозрачность услуг.

После дерегуляции в 1980-х годах, когда рынок стал более открытым и конкурентным, регулирование переместилось в сторону безопасности и контроля за операторами. Значимым этапом стало создание Федерального управления по безопасности автотранспорта (FMCSA), которое ввело формальные требования к лицензированию, безопасности автопарка, ведению отчётности и защите прав потребителей. Параллельно в отрасли начали формироваться частные стандартизированные сервисные модели, разработанные сетевыми компаниями и франчайзерами.

С конца XX – начала XXI века стандартизация стала основным инструментом консолидации рынка. Крупные федеральные франчайзинговые сети внедрили детализированные операционные процедуры, корпоративные стандарты обслуживания,

аудиторские механизмы и систему внутреннего комплаенса. Это позволило унифицировать качество услуг по всей стране и обеспечить масштабирование бизнеса без потери операционной стабильности.

Сегодня стандартизация и комплаенс представляют собой комплекс норм, включающий требования федеральных регуляторов, внутренние корпоративные регламенты и отраслевые best practices. Их историческое развитие отражает переход от минимального государственного контроля к интегрированной модели, где соблюдение стандартов является ключевым условием доверия клиентов, безопасности операций и устойчивости франчайзинговых сетей (табл. 1) [2].

**Таблица 1 – Стандартизация и комплаенс**

| № | Стандартизация                                                                                                                                                                       | Комплаенс                                                                                                                                                                                                |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | <i>Определение стандартов.</i> Создание единых процедур и требований для всех участников логистической цепи, включая транспорт, складирование, упаковку и обработку грузов.          | <i>Соблюдение законодательства.</i> Комплаенс подразумевает выполнение всех применимых законов и норм, касающихся логистики, включая таможенные правила, правила безопасности и охраны окружающей среды. |
| 2 | <i>Международные стандарты.</i> Применение стандартов ISO (например, ISO 9001 для систем менеджмента качества) и других международных норм, таких как GS1 для идентификации товаров. | <i>Мониторинг и контроль.</i> Внедрение систем мониторинга для отслеживания соблюдения стандартов и требований, а также регулярные аудиты и проверки.                                                    |
| 3 | <i>Упрощение процессов.</i> Стандарты помогают унифицировать процессы, что снижает риски ошибок и повышает производительность.                                                       | <i>Обучение персонала.</i> Обучение сотрудников требованиям комплаенса и стандартам, чтобы гарантировать их понимание и выполнение.                                                                      |

Отметим, что современная мувинговая индустрия США характеризуется высокой степенью стандартизации и развитой системой комплаенса, что делает возможным быстрое и контролируемое масштабирование бизнеса через франчайзинг.

Крупные сети, такие как Two Men and a Truck, College Hunks Hauling Junk & Moving, Allied Van Lines и Mayflower, активно внедряют унифицированные операционные платформы, что позволяет выровнять качество обслуживания между франчайзи и корпоративными филиалами.

По данным IBISWorld и American Moving and Storage Association, более 80% крупных сетевых перевозчиков используют централизованные CRM и платформы управления рабочей силой, обеспечивая единую стандартизацию процессов. В сетях с развитой цифровой инфраструктурой разница в клиентских оценках между филиалами снижается до 5-7%, тогда как у компаний без единых систем разброс превышает 20%.

Использование интегрированных систем расписания и GPS-мониторинга позволило сократить среднее время прибытия экипажей на 12-18%, а автоматизированные модули расчёта стоимости уменьшили количество ошибок в кватировании на 25-30%. Единые стандарты аудита качества, применяемые в Allied Van Lines и Mayflower, привели к росту показателя удовлетворенности клиентов до 90-92%, что на 10 пунктов выше среднего по рынку независимых перевозчиков.

В основе их модели лежат детализированные операционные руководства, включающие стандарты обучения персонала, требования к технике и оснащению, правила упаковки и погрузки, унифицированные чек-листы качества, алгоритмы взаимодействия с клиентом и сценарии коммуникации. Эти стандарты подкреплены цифровыми платформами, которые позволяют централизованно управлять заказами, логистикой, расписанием экипажей и контролем KPI [1].

Комплаенс в отрасли основывается на строгих требованиях FMCSA, включающих обязательную регистрацию перевозчиков, получение DOT-номера, поддержание страховых полисов установленного уровня, соблюдение норм Hours of Service и ведение электронных логбуков. Франчайзинговые сети интегрируют выполнение этих требований в свои внутренние регламенты, чтобы обеспечить соответствие федеральным стандартам для каждого франчайзи. Регулярные внутренние аудиты, анализ записи телематики, проверка состояния автопарка, контроль страховых и верификация бухгалтерской отчётности входят в обязательный цикл комплаенса (рис. 1).



Рис. 1 – Основные аспекты стандартизации и комплаенс-функций [3]

Дополнительно сети применяют собственные стандарты корпоративного качества, например обязательное прохождение сервисной сертификации, соблюдение визуального стандарта бренда, регламентов по работе с жалобами и обслуживанию клиентов. Многие компании используют программы «тайный клиент» и автоматические NPS-опросы, что создаёт цифровой след, необходимый для точной оценки работы каждого подразделения. Благодаря такой системе франчайзи получают готовую операционную экосистему, где процессы заранее описаны и проверены, а соблюдение требований обеспечивается через регулярные инспекции и централизованные информационные панели.

Данная модель стандартизации и комплаенса делает возможным быстрое расширение сети без потери качества, снижает операционные риски и повышает доверие потребителей. В результате рынок мувинговых услуг в США демонстрирует устойчивую тенденцию к консолидации вокруг крупных франчайзинговых брендов, которые используют стандартизированные процессы как стратегическое преимущество и основу масштабируемости.

Следует подчеркнуть, что мувинговая индустрия США сталкивается с рядом системных трудностей, которые делают стандартизацию и комплаенс неполными и неоднородными, даже внутри крупных франчайзинговых сетей.

Главная проблема – *высокая фрагментация рынка*, где значительную долю занимают малые независимые перевозчики. Это усложняет выработку единых отраслевых правил и приводит к тому, что стандарты крупных сетей зачастую не совпадают с практиками остальных игроков. В условиях масштабирования через франчайзинг это создаёт сложность поддержания стабильного уровня сервиса, так как новые франчайзи могут приходить с собственными привычками, отличающимися от корпоративных регламентов.

Серьёзной проблемой остается *комплаенс с требованиями FMCSA*. Несмотря на стандартизированные процедуры, франчайзи нередко допускают нарушения, связанные с техническим состоянием автомобилей, ведением электронных логов, страховыми полисами и правилами безопасности водителей. Компании вынуждены тратить ресурсы на постоянные аудиты и мониторинг, но контроль остаётся несовершенным, особенно в подразделениях, работающих в удаленных регионах. Несогласованность локальной практики и федеральных норм приводит к рискам штрафов, судебных разбирательств и репутационным потерям.

Сложность вызывает и *стандартизация операционных процессов*. Даже при наличии подробных руководств выполнение регламентов зависит от дисциплины экипажа и менеджмента. В мувинге значительную роль играют человеческие факторы – качество упаковки, аккуратность погрузки, работа с клиентом. Эти процессы трудно полностью формализовать, что приводит к разрыву в качестве между разными франчайзи. Дополнительную проблему создаёт высокая текучка кадров: постоянное обучение новых сотрудников становится дорогим и затрудняет обеспечение единых стандартов.

Также существуют трудности с *цифровой стандартизацией*. Франчайзинговые сети внедряют обязательные CRM-системы, трекинг и аналитику, но франчайзи не всегда корректно используют технологические инструменты. Это приводит к неточности данных, невозможности контролировать KPI и снижению эффективности всей сети. Некоторые регионы требуют адаптации процессов из-за разницы в законодательстве штатов, что усложняет создание единой операционной модели.

Остаётся значимой и проблема *бренда*. Нарушения стандартов в одном подразделении наносят ущерб всей сети. Даже при наличии строгих правил часть франчайзи пытается экономить на обучении, экипировке, страховках или автопарке. Это приводит к неравномерности качества услуг, что противоречит ключевому принципу франчайзинга – предсказуемости и стабильности.

В итоге стандартизация и комплаенс в мувинговой индустрии США сталкиваются с комплексом препятствий: несогласованность отрасли, вариативность выполнения регламентов, трудности контроля, человеческий фактор, различия региональных норм и неполная цифровизация. Все эти проблемы усложняют построение идеально масштабируемой модели, требуя от франчайзинговых сетей постоянных инвестиций в мониторинг, обучение, технологии и внутренний контроль.

По нашему мнению, эффективное решение проблем стандартизации и комплаенса в мувинговой индустрии США требует сочетания технологической унификации, усиленного операционного контроля и системной работы с франчайзи.

Одним из ключевых шагов становится создание единой цифровой экосистемы, обязательной для всех подразделений без исключений. Централизованная CRM, единая система расчёта стоимости, мобильные приложения для экипажей, автоматический трекинг транспорта и цифровые чеклисты позволяют снижать вариативность исполнения, фиксировать статистику в реальном времени и исключать человеческие ошибки. Стандартизация через технологии обеспечивает прозрачность работы франчайзи и создаёт основу для регулярного автоматизированного аудита, что значительно повышает уровень комплаенса.

Важным направлением становится унификация процедур обучения. Компании внедряют обязательные многоуровневые программы сертификации сотрудников, виртуальные тренажёры, видео-инструкции, регулярные тестирования и контроль качества обучения. Такой подход позволяет нивелировать влияние высокой текучки и обеспечить единый уровень профессиональных навыков в разных локациях. Дополнительные выездные аудиты и «тайные клиенты» позволяют выявлять отклонения от стандартов и оперативно корректировать работу персонала.

Для усиления комплаенса с требованиями FMCSA и страховых регуляторов применяется централизованное управление автопарком. Вводятся обязательные стандарты технического обслуживания, регулярные проверки состояния транспорта, мониторинг ELD-логов, автоматическое уведомление о нарушениях и санкции для франчайзи, не соблюдающих минимальные требования безопасности. Это снижает риски штрафов, ДТП и судебных претензий, одновременно поддерживая единый уровень операционной дисциплины.

Франчайзинговые сети усиливают контроль за качеством, внедряя систему KPI, которая напрямую влияет на роялти, бонусы и доступ к маркетинговой поддержке. Показатели включают рейтинг клиентов, процент рекламаций, соблюдение стандартов упаковки, точность расчёта стоимости, выполнение временных норм и количество нарушений комплаенса. Такой механизм выравнивает мотивацию франчайзи и заставляет их придерживаться корпоративных стандартов, поскольку несоблюдение норм начинает напрямую отражаться на финансовых результатах.

Значимую роль играет юридическая стандартизация. Франчайзинговые соглашения дополняются жёсткими положениями о соблюдении бренда, использовании единой айдентики, обязательных операционных требований и санкционными мерами за отклонения. При этом компании предоставляют франчайзи шаблоны локальной документации, стандартизированные страховые решения, рекомендации по соблюдению законов штатов и доступ к юридической поддержке, что снижает несогласованность практик между регионами.

В итоге комплексное решение проблем стандартизации и комплаенса достигается за счёт цифровой унификации, многоканального контроля, обязательной сертификации персонала, централизованного комплаенс-менеджмента и жёсткой регуляции в рамках франчайзинговой модели. Такой подход позволяет создать масштабируемую, предсказуемую и управляемую операционную сеть даже в условиях высокой фрагментации мувингового рынка США.

**Заключение.** Комплаенс в мувинговой индустрии имеет стратегическое значение, поскольку напрямую связан с безопасностью перевозок, регулированием FMCSA, страховыми обязательствами и репутационными рисками. Внедрение строгих процедур,

регулярных проверок, отслеживания нарушений и обязательных корректирующих действий формирует культуру ответственности, которая становится ключевым конкурентным преимуществом бренда. Франчайзи, получающие чёткие инструкции, инструменты, обучение и поддержку, способны поддерживать нужный уровень качества, а франчайзер – контролировать и оперативно реагировать на любые отклонения.

Таким образом, стандартизация и комплаенс являются не ограничениями, а мощным механизмом роста. Они позволяют бизнесу создавать предсказуемый клиентский опыт, снижать операционные издержки, повышать доверие потребителей и обеспечивать стабильность сети. Компании, которые сумеют интегрировать технологии, процедуры и культуру контроля в единую систему, получают возможность масштабироваться быстрее конкурентов и закрепляться на новых рынках с минимальными рисками.

### Список литературы:

1. Гайнутдинова М.Т. Аутсорсинг логистических услуг // Экономика и социум. – №5-1 (72). – 2020. – С. 473-477.
2. Минаков А.В. Роль транспортной логистики в развитии экономики региона // Экономика и бизнес: теория и практика. – №12-1 (118). – 2024. – С. 168-175.
3. Селезнева М.М. Новое руководство по выстраиванию комплаенс-функции // Экономика и бизнес: теория и практика. – №(2). – 2015. – С. 68-71.

## ТЕХНИКАЛЫҚ ҒЫЛЫМДАР - ТЕХНИЧЕСКИЕ НАУКИ - TECHNICAL SCIENCE

UDC 37.013.3:331.5

**Dauletbay Assiyat Bagdatkyzy,****Shamil Nartay Muratuly,****Serikov Mansur Kuanyshpayevich**

Students  
of the Educational Program “Software Engineering”  
(Astana, Kazakhstan)

**Scientific supervisor:** Kazhybayev Olzhas**FROM CLASSROOM TO CAREER: LEVERAGING PEER-TO-PEER SKILL  
EXCHANGE TO REDUCE THE EMPLOYABILITY GAP**

**Abstract:** The employability gap, commonly defined as the mismatch between graduates’ skills and labor market expectations, remains a persistent challenge for higher education institutions worldwide. While universities increasingly emphasize employability, many existing interventions are resource-intensive, unevenly accessible, or difficult to scale. This review article explores the potential of peer-to-peer (P2P) skill exchange as a complementary and scalable approach to reducing the employability gap among university students. Drawing on existing literature on employability frameworks, skills mismatch, and peer-based learning, the article identifies key mechanisms through which P2P skill exchange may enhance employability, including skills practice and transfer, feedback and communication development, social capital formation, and self-efficacy. The paper also outlines practical design considerations for implementing P2P skill exchange initiatives in higher education and highlights directions for future research focused on evaluating employability outcomes.

**Keywords:** employability; peer-to-peer learning; skill exchange; higher education; skills mismatch; career readiness; peer mentoring

**Setting the problem: why the employability gap persists**

Graduate employability is increasingly shaped by rapid skill change, rising expectations for “work-ready” evidence, and unequal access to experiential learning. Major skills outlooks emphasise that labour-market outcomes are strongly associated with disparities in cognitive, digital and socio-emotional skills, and that resilience depends on continuous upskilling rather than one-off credential attainment. Employer-facing forecasts also anticipate significant job and skill disruption through 2030, with growing demand for analytical thinking, technology literacy, and human skills such as collaboration and leadership.

In parallel, employability scholarship has moved beyond “employment rates” toward models that integrate competence, reflection, identity, and opportunity structures. A systematic review of employability models in higher education shows substantial variation in how employability is defined and taught, but converges on the idea that employability requires (i) capability and (ii) the ability to evidence that capability in contexts that matter to employers.

Universities have expanded employability interventions—career services, skills modules, mentoring, and work-integrated learning—but these are often resource-intensive and unevenly accessed. This creates a design challenge: how can institutions increase employability development opportunities at scale while mitigating inequality of participation and outcomes?

### **Literature review: what we know about peer learning and employability**

#### **Employability as capability + evidence**

Recent syntheses argue that employability development depends on the integration of competence development with reflective and evidencing processes that help students translate learning into credible signals for employers. This “capability + evidence” framing is useful because many employability gaps are not purely about lacking skills; they are also about lacking structured opportunities to practice, receive feedback, and produce demonstrable outputs.

#### **Peer learning as an employability and equity lever**

Peer learning has been positioned as a means to foster social mobility and employability, including reducing attainment gaps and differentials in employment outcomes. Donald and Ford argue that peer learning can contribute to employability by strengthening engagement, belonging, and skill development while creating scalable support structures. In practice, institutions have begun embedding peer learning across curricula and co-curricular ecosystems to broaden access and normalise participation.

#### **Peer feedback and peer assessment as “feedback literacy” training**

A growing body of work examines peer feedback and peer assessment as structured ways to build evaluative judgement and communication skills. A systematic review of online peer feedback practices (higher education) synthesises evidence on what makes peer feedback effective and how design choices influence learning outcomes. Complementary work on designing peer assessment processes reports strong evidence that formative peer feedback—where students can apply feedback—supports performance and learning, reinforcing the employability-relevant capacity to give, receive and use feedback.

#### **Peer learning in employability-focused sessions**

Empirical work also examines peer learning within employability teaching. A 2024 study of peer-focused employability learning experiences reports how students “gain from peers” via comparison, reflection, and collaborative sense-making—processes linked to career identity and employability learning.

#### **Where “P2P skill exchange” fits**

Peer-to-peer skill exchange can be conceptualised as a structured extension of peer learning: rather than general peer support, students explicitly offer and request skills (e.g., data analysis ↔ presentation design; interview practice ↔ English for workplace communication). In the 2020–2025 literature, fully evaluated university-wide P2P exchange models remain limited; however, platform prototypes and institutional initiatives exist, suggesting feasibility and pointing to design issues (matching, quality assurance, recognition).

Separately, policy work on employability skills gaps emphasises the need for scalable strategies that strengthen practical competencies and work-relevant behaviours, particularly where formal work placements are limited.

#### **Methodological approach: rapid scoping synthesis**

This article uses a rapid scoping synthesis to map and integrate 2020–2025 literature across four strands: (i) employability models, (ii) peer learning and employability, (iii) peer feedback/assessment design, and (iv) P2P skill exchange initiatives and prototypes. Scoping

approaches are appropriate for emerging topics where evidence is heterogeneous and the objective is to identify mechanisms, design principles, and research gaps rather than produce pooled effect sizes.

Reporting follows contemporary guidance for transparent evidence synthesis using PRISMA 2020 (for reporting discipline and traceability of selection and synthesis steps).

Inclusion logic (high-level): sources (a) published 2020–2025, (b) focused on higher education or graduate employability/skills policy, and (c) contained explicit relevance to peer learning/peer feedback or P2P skill exchange mechanisms.

Synthesis method: thematic synthesis was used to derive mechanism pathways (how P2P exchange could plausibly influence employability) and implementation/evaluation implications, triangulating across empirical findings, systematic reviews, and institutional practice accounts.

Results: five mechanisms linking P2P skill exchange to employability

### **1) Skills practice at scale (competence building through reciprocal teaching/learning)**

P2P exchange increases opportunities for repeated practice and explanation. This matters because contemporary skills outlooks stress that employability is increasingly shaped by adaptable, practice-based competence (not just credential possession). Skill exchange structures also encourage cross-disciplinary learning—useful when job roles blend technical and human skills.

### **2) Feedback literacy and professional communication**

Peer exchange naturally embeds feedback cycles: learners state goals, peers observe outputs, and feedback is discussed and applied. Evidence from peer feedback research shows that design (clarity, purpose, and the ability to apply feedback) is critical to learning benefits—suggesting that P2P exchange should be scaffolded with simple feedback templates and reflection prompts.

### **3) Social capital and opportunity awareness**

Peer learning has been argued to support employability partly by improving belonging, retention, and bridging differentials that affect outcomes—especially important for social mobility. P2P exchange can widen students' networks across cohorts and disciplines, making opportunity information (projects, competitions, internships) more visible and accessible.

### **4) Career identity, confidence, and self-efficacy**

Peer-focused employability sessions show that students gain from peers by comparing experiences, recognising shared concerns, and refining career narratives—processes tied to career identity development. In P2P skill exchange, students can experience “micro-wins” (teaching a skill successfully; completing a mini-project) that strengthen confidence and readiness to perform in selection contexts.

### **5) Stronger signalling through artefacts (portfolios, micro-evidence, peer-review traces)**

Employability models emphasise that employability is partly about translating learning into credible signals. P2P exchange is especially suited to producing tangible artefacts: mini-projects, peer-reviewed outputs, feedback logs, and portfolio entries. These artefacts can be aligned with skills employers prioritise (e.g., analytical thinking, tech literacy, leadership) as highlighted in workforce outlooks.

Implications for practice: how universities can implement P2P skill exchange

### **Programme architecture (minimum viable model):**

- Offer/Request catalogue: students list teachable skills and desired skills using a controlled taxonomy aligned with current skills outlook categories.
- Matching rules: match by level, schedule, language, and goals (skill outcome + artefact target).
- Session structure: 30–60 minutes with a defined output (e.g., revised CV bullet, solved task, mini-prototype).
- Feedback scaffold: short rubric + “actionable feedback” template (what worked / what to improve / next step), reflecting peer feedback design evidence.

#### **Quality assurance:**

- brief onboarding for peer mentors/tutors (how to explain, set goals, and give feedback)
- moderation via ratings + random audits of artefacts (lightweight)
- escalation paths for misconduct or low-quality patterns

#### **Equity design:**

Peer learning can reduce differentials only if participation is broad and supported. Universities should proactively recruit less-represented cohorts, provide “starter exchanges” (low-stakes, beginner-friendly), and support scheduling/access for students with work or caregiving responsibilities.

#### **Recognition:**

A co-curricular record or internal badge can document hours + artefacts, but institutions should avoid overstating credential equivalence unless external validation exists.

#### **Evaluation framework: measuring impact without overclaiming**

To move beyond “participation counts,” evaluation should include:

- Skill gains: pre/post self-ratings + short performance tasks; peer feedback quality indicators (structure, specificity).
- Employability development: measures aligned with employability model constructs identified in systematic reviews (e.g., reflection, evidence articulation, confidence).
- Equity analytics: uptake and retention by programme, gender, socioeconomic indicators (where ethically and legally possible).
- Artefact outcomes: number and quality of portfolio items, mini-projects, peer-review traces.
- Longitudinal outcomes: internships/interviews/early employment indicators, interpreted cautiously given labour-market variance highlighted in skills outlooks.

| Dimension     | Indicator              | Data source           |
|---------------|------------------------|-----------------------|
| Skill gains   | Pre/post task          | Short assessment      |
| Employability | Confidence, reflection | Survey                |
| Equity        | Uptake by cohort       | Admin data            |
| Artefacts     | Portfolio quality      | Rubric                |
| Outcomes      | Internships            | Longitudinal tracking |

**Conclusion.** Evidence from 2020–2025 literature supports the plausibility that peer learning can foster employability and social mobility, and that well-designed peer feedback processes build communication and evaluative judgement relevant to work. This review extends that line of reasoning to P2P skill exchange, identifying five mechanism pathways—scaled practice, feedback literacy, social capital, career identity/self-efficacy, and improved signalling through artefacts—through which P2P exchange may reduce employability gaps.

However, the empirical evidence base specifically evaluating university-wide P2P skill exchange remains thin relative to broader peer learning research, indicating a clear research opportunity. Future studies should prioritise: (1) quasi-experimental evaluations comparing participants with matched non-participants, (2) equity-focused analyses of who participates and benefits, and (3) employer-side studies testing how P2P-generated artefacts and peer-review traces influence hiring judgments. In the context of accelerating skill disruption, scalable, evidence-generating models such as P2P exchange merit serious institutional experimentation.

### References:

1. Chilvers, L. (2025). A UK institution's approach to broadening and embedding peer learning and support. *Journal of Peer Learning*.
2. Christie, F. (2024). An exploration of the impact of different peer learning interactions on student learning in peer-focused employability experiences. *Teaching in Higher Education*.
3. Donald, W. E., & Ford, N. (2023). Fostering social mobility and employability: The case for peer learning. *Teaching in Higher Education*.
4. Eimer, A., & Bohndick, C. (2023). Employability models for higher education: A systematic literature review and analysis. *Social Sciences & Humanities Open*.
5. Gao, X., et al. (2024). A systematic review of the key components of online peer feedback practices in higher education. *Educational Research Review*.
6. International Labour Organization. (2022). Bridging the employability skills gap in higher education. ILO.
7. OECD. (2021). A new approach to skills mismatch. OECD Publishing.
8. OECD. (2023). OECD Skills Outlook 2023. OECD Publishing.
9. Page, M. J., McKenzie, J. E., Bossuyt, P. M., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71.
10. World Economic Forum. (2023). The Future of Jobs Report 2023. World Economic Forum.
11. World Economic Forum. (2025). The Future of Jobs Report 2025. World Economic Forum.
12. Fleckney, P. (2025). Designing effective peer assessment processes in higher education. *Higher Education Research & Development*.
13. Othman, F. (2023). PeerLoom: Peer-to-peer skill exchange platform for students (Institutional repository project).

УДК 621.7.04

**Нажим Танат Муратулы**

Магистрант кафедры «Технологические машины и оборудование»  
Казахский агротехнический исследовательский университет  
(г. Астана, Казахстан)

**Научный руководитель:** Мендалиева Сауле Ильинична

## **АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ ТОЧНОСТИ В ТЕХНОЛОГИИ FDM-печати**

**Аннотация:** В этой статье рассматривается анализ методов обеспечения размерной точности деталей, послойного наращивания FDM (Fused Deposition Modeling). Исследованы факторы, приводимые к погрешностям, возникающим в процессе FDM-печати, включая технологические, механические, термические и программные причины. Выполнен обзор влияния параметров печати, таких как высота слоя, температурные режимы, ориентация детали и скорость экструзии, на геометрическую точность деталей. Анализируются существующие методы повышения точности FDM-деталей, в том числе охватывая технологические и конструктивные подходы, программную настройку и геометрическую компенсацию размерных отклонений на этапе проектирования. Выполнено краткое сравнение технологии FDM с другими аддитивными методами по показателям точности.

**Ключевые слова:** FDM-печать, 3D-печать, погрешности изготовления

Создание трёхмерных предметов через послойное осаждение материала - так работает 3D-печать, основанная на цифровых моделях [1]. Эта методика входит в категорию аддитивных производственных способов, иногда её называют быстрым прототипированием. Наиболее часто применяют именно FDM-подход среди прочих вариантов [2]. Недорогие станки, устойчивость готовых деталей к изнашиванию, выбор сырья, приемлемая длительность изготовления - всё это характерно для FDM [3]. Точность геометрических параметров и текстура внешних сторон оставляют желать лучшего при использовании этой технологии [4]. Из-за способа нанесения материала послойно, на изделиях, созданных методом FDM, обычно видны переходы между уровнями. Вблизи детализированных участков возможны отклонения в геометрии. Следовательно, технология не всегда подходит для элементов, где важна тонкая передача формы.

FDM-технология относится к аддитивным методам, основанным на экструзии расплавленного термопластика по заранее заданной траектории. В основе технологии лежит принцип последовательного нанесения расплавленного полимерного материала в виде отдельных слоёв по заданной траектории, формируемой на основе трёхмерной цифровой модели изделия [5, 6]. Цифровая модель, как правило, создаётся в CAD-системах и затем преобразуется в управляющий код с использованием программ слайсинга, в которых задаются основные параметры печати.

Процесс FDM-печати состоит из этапов подготовки цифровой модели, её слайсинга, экструзии материала и послойного наращивания, сопровождающихся охлаждением и кристаллизацией полимера. Особенностью технологии является дискретный характер

формирования изделия, что напрямую влияет на точность воспроизведения геометрических элементов, особенно в направлении оси Z, а также на качество поверхностей и сопряжений [5, 6].

FDM-технология получила широкое распространение благодаря доступности оборудования и возможности работы с различными термопластиками. Наиболее часто применяемыми материалами являются PLA, ABS, PETG, полиамиды и композитные филаменты, свойства которых существенно влияют на стабильность процесса печати и формирование размерных отклонений [7, 8]. В научных исследованиях отмечается, что физико-механические и термические характеристики используемых материалов оказывают значительное влияние на усадку, деформации и адгезию между слоями, что в конечном итоге отражается на точности изготавливаемых деталей [7, 14, 15].

Области применения FDM-технологии охватывают быстрое прототипирование, изготовление опытных образцов, функциональных деталей малых серий, а также вспомогательной оснастки и приспособлений. Однако при расширении области применения FDM-печати в инженерных и промышленных задачах всё более актуальной становится проблема обеспечения стабильной размерной и геометрической точности изделий [9, 10]. В ряде работ подчёркивается, что без применения специальных методов оптимизации технологических параметров и компенсации погрешностей технология FDM уступает другим аддитивным методам по показателям точности [9, 16, 18].

Таким образом, технология FDM представляет собой эффективный и универсальный инструмент аддитивного производства, обладающий значительным потенциалом применения. Вместе с тем, присущие ей технологические и физические ограничения обуславливают необходимость комплексного анализа факторов, влияющих на точность изготовления деталей, а также разработки и систематизации методов её обеспечения, что и определяет актуальность дальнейших исследований в данной области.

Обеспечение размерной и геометрической точности деталей, изготовленных методом FDM-печати, осложняется наличием комплекса погрешностей, формирующихся на различных этапах технологического процесса. Согласно результатам многочисленных исследований, итоговая погрешность изделия имеет системный характер и обусловлена совместным воздействием механических, термических, технологических и программных факторов [5, 9, 11].

Механические погрешности связаны с конструктивными особенностями 3D-принтеров и точностью их кинематических систем. К основным причинам относятся люфты в направляющих и приводах, неточность позиционирования шаговых двигателей, а также недостаточная жёсткость несущих элементов оборудования. Данные факторы приводят к отклонениям фактической траектории движения экструдера от заданной, что особенно критично при формировании контуров и сопрягаемых поверхностей [12, 13].

Термические погрешности обусловлены процессами охлаждения и усадки термопластичного материала после экструзии. Неравномерное распределение температуры по объёму изделия вызывает внутренние напряжения, приводящие к линейным и объёмным деформациям, а также к короблению изделия. Наибольшее влияние данные эффекты оказывают при использовании материалов с высокой термической усадкой и при печати деталей значительных габаритов [7, 14, 15].

Значительную роль в формировании погрешностей играют параметры технологического процесса FDM-печати. Высота слоя, скорость экструзии, температура

сопла и рабочей платформы, плотность заполнения и ориентация детали в рабочей зоне оказывают прямое влияние на точность геометрии и качество поверхности изделия. Дискретный послойный характер формирования деталей приводит к ступенчатости поверхностей и снижению точности воспроизведения криволинейных элементов, особенно по оси Z [16–18].

Программные погрешности формируются на этапах подготовки цифровой модели и слайсинга. Аппроксимация геометрии треугольной сеткой STL-формата, особенности алгоритмов генерации траекторий, а также округление координат приводят к систематическим отклонениям размеров. Ряд исследований указывает на возможность компенсации данных погрешностей путём оптимизации параметров слайсера и применения методов геометрической коррекции цифровых моделей [19, 20].

Повышение точности деталей, изготавливаемых методом FDM-печати, является комплексной научно-технической задачей, требующей одновременного учёта конструктивных особенностей оборудования, свойств применяемых материалов, параметров технологического процесса и алгоритмов подготовки цифровых моделей. В современных исследованиях методы обеспечения точности принято классифицировать по этапам жизненного цикла изделия: на этапе проектирования, подготовки управляющих программ, непосредственно в процессе печати и на этапе постобработки [9, 10, 16].

Одним из наиболее распространённых и доступных методов повышения точности является оптимизация параметров FDM-печати. Исследования показывают, что высота слоя, скорость экструзии, температура сопла и рабочей платформы оказывают определяющее влияние на точность размеров и качество поверхности деталей [16–18]. Снижение высоты слоя позволяет уменьшить ступенчатость поверхностей и повысить точность по оси Z, однако приводит к увеличению времени печати.

Температурные параметры определяют вязкость расплава и условия межслойной адгезии. Недостаточная температура экструзии может вызывать неполное сплавление слоёв, тогда как чрезмерная температура способствует деформациям и ухудшению геометрической стабильности изделия. В научных работах подчёркивается, что оптимальные режимы печати должны подбираться индивидуально для каждого материала и геометрии детали [7, 14, 16].

**Таблица 1 - Влияние основных параметров FDM-печати на точность изделий**

| Параметр          | Направление влияния          | Эффект на точность                        |
|-------------------|------------------------------|-------------------------------------------|
| Высота слоя       | Уменьшение                   | Повышение точности и качества поверхности |
| Скорость печати   | Уменьшение                   | Снижение динамических погрешностей        |
| Температура сопла | Оптимизация                  | Улучшение межслойной адгезии              |
| Температура стола | Повышение (в пределах нормы) | Снижение коробления                       |
| Ориентация детали | Оптимальный выбор            | Снижение анизотропии погрешностей         |

Эффективным методом обеспечения точности является предварительная геометрическая компенсация цифровых моделей. Суть данного подхода заключается во внесении целенаправленных изменений в CAD-модель с учётом ожидаемых деформаций и усадки материала в процессе печати. Такие методы позволяют компенсировать систематические погрешности, обусловленные физическими свойствами материала и особенностями оборудования [19, 20].

В ряде исследований показано, что применение масштабных коэффициентов и локальных геометрических корректировок позволяет существенно снизить отклонения линейных размеров без изменения параметров технологического процесса. Наиболее эффективно данный подход применяется при серийном изготовлении однотипных деталей, где характер погрешностей является воспроизводимым [12, 20].

Отдельную группу методов составляют аппаратные и конструктивные способы повышения точности FDM-печати. К ним относятся повышение жёсткости рамы принтера, использование высокоточных линейных направляющих, калибровка кинематических узлов и применение систем автоматической коррекции положения платформы [12, 13].

Современные исследования также рассматривают внедрение систем обратной связи, основанных на датчиках температуры, положения и скорости перемещения экструдера. Использование таких систем позволяет снизить влияние случайных и динамических погрешностей и обеспечить более стабильное качество изготавливаемых деталей [9].

**Таблица 2 — Аппаратные методы повышения точности FDM-печати**

| Метод                                       | Принцип действия                       | Результат                           |
|---------------------------------------------|----------------------------------------|-------------------------------------|
| Калибровка кинематики                       | Устранение люфтов и перекосов          | Повышение точности позиционирования |
| Усиление рамы                               | Повышение жёсткости конструкции        | Снижение вибраций                   |
| Автоматическая калибровка рабочей платформы | Коррекция плоскостности                | Стабильность первого слоя           |
| Системы обратной связи                      | Контроль параметров в реальном времени | Снижение случайных погрешностей     |

Анализ научных публикаций показывает, что наибольший эффект в обеспечении точности достигается при комплексном применении различных методов. Использование только оптимизации параметров печати без учёта программных и аппаратных факторов не позволяет полностью устранить систематические погрешности. В связи с этим в современных работах всё чаще рассматриваются интегрированные подходы, сочетающие оптимизацию режимов печати, геометрическую компенсацию и аппаратную коррекцию процесса [10, 16, 18].

Таким образом, методы обеспечения точности в технологии FDM-печати представляют собой многоуровневую систему технических и программных решений, выбор и эффективность которых зависят от требований к изделию, используемых материалов и условий производства.

### Список литературы:

1. Зленко М. А., Нагайцев М. В., Довбыш В. М. Аддитивные технологии в машиностроении : пособие для инженеров / М. А. Зленко, М. В. Нагайцев, В. М. Довбыш. — М. : ГНЦ РФ ФГУП «НАМИ», 2015. — 220 с.
2. Петров А. Н., Смирнова И. В. Методы повышения точности 3D-печати методом FDM // Вестник машиностроения и материаловедения. — 2021. — Т. 9, № 2. — С. 112–120.

3. Михальченко А. А. Исследование качества деталей из различных видов пластика, изготовленных методом FDM-печати / А. А. Михальченко // Исследования и разработки в области машиностроения, энергетики и управления : материалы XXII Междунар. науч.-техн. конф. студентов, аспирантов и молодых ученых (Гомель, 28–29 апр. 2022 г.) / под общ. ред. А. А. Бойко. — Гомель : ГГТУ им. П. О. Сухого, 2022. — С. 99–101.
4. Güler T., Demirci E., Yıldız A. R., Yavuz U. Lightweight design of an automobile hinge component using glass fiber polyamide composites // *Materials Testing*. — 2018. — Т. 60, № 3. — С. 306–310.
5. Gibson I., Rosen D., Stucker B. *Additive Manufacturing Technologies: 3D Printing, Rapid Prototyping, and Direct Digital Manufacturing*. — Springer, 2021. — 520 с.
6. Chua C. K., Leong K. F., Lim C. S. *Rapid Prototyping: Principles and Applications*. — World Scientific Publishing, 2019. — 360 с.
7. Sun Q., Rizvi G. M., Bellehumeur C. T., Gu P. Effect of processing conditions on the bonding quality of FDM polymer filaments // *Rapid Prototyping Journal*. — 2008. — Т. 14, № 2. — С. 72–80.
8. Torrado Perez A. R., Roberson D. A., Wicker R. B. Fracture surface analysis of 3D-printed ABS-based materials // *Journal of Failure Analysis and Prevention*. — 2014. — Т. 14. — С. 343–353.
9. Turner B. N., Strong R., Gold S. A. A review of melt extrusion additive manufacturing processes: I. Process design and modeling // *Rapid Prototyping Journal*. — 2014. — Т. 20, № 3. — С. 192–204.
10. Ngo T. D., Kashani A., Imbalzano G., Nguyen K. T. Q., Hui D. Additive manufacturing (3D printing): A review of materials, methods, applications and challenges // *Composites Part B*. — 2018. — Т. 143. — С. 172–196.
11. Ahn S. H., Montero M., Odell D., Roundy S., Wright P. K. Anisotropic material properties of fused deposition modeling ABS // *Rapid Prototyping Journal*. — 2002. — Т. 8, № 4. — С. 248–257.
12. Boschetto A., Bottini L. Accuracy prediction in fused deposition modeling // *The International Journal of Advanced Manufacturing Technology*. — 2014. — Т. 73. — С. 913–928.
13. Galantucci L. M., Lavecchia F., Percoco G. Experimental study aiming to enhance the surface finish of fused deposition modeled parts // *CIRP Annals*. — 2009. — Т. 58, № 1. — С. 189–192.
14. Bellehumeur C. T., Li L., Sun Q., Gu P. Modeling of bond formation in the fused deposition modeling process // *Journal of Manufacturing Processes*. — 2004. — Т. 6, № 2. — С. 170–178.
15. Spoerk M., et al. Shrinkage and warpage behavior of FDM printed parts // *Polymer Engineering & Science*. — 2017. — Т. 57, № 7. — С. 753–763.
16. Mohamed O. A., Masood S. H., Bhowmik J. L. Optimization of fused deposition modeling process parameters: A review // *Materials & Design*. — 2015. — Т. 83. — С. 906–917.
17. Sood A. K., Ohdar R. K., Mahapatra S. S. Parametric appraisal of mechanical properties of fused deposition modeling processed parts // *Materials & Design*. — 2010. — Т. 31, № 1. — С. 287–295.

18. Peng A., Xiao X., Yue R. Process parameter optimization for improving dimensional accuracy in fused deposition modeling // *Procedia Manufacturing*. — 2019. — Т. 30. — С. 373–380.
19. Pandey P. M., Reddy N. V., Dhande S. G. Slicing procedures in layered manufacturing: A review // *Computer-Aided Design*. — 2003. — Т. 35, № 4. — С. 297–317.
20. Boschetto A., Giordano V. Geometrical accuracy improvement of FDM parts through model modification // *Precision Engineering*. — 2013. — Т. 37, № 4. — С. 851–859.

УДК 347.1

**Khassanov Fakhreddin**

Master's student  
Kazakh University of Technology and Business named after K. Kulazhanov  
(Astana, Kazakhstan)

**Shaikhanova Aigul**

Ph.D, associate professor  
Kazakh University of Technology and Business named after K. Kulazhanov  
(Astana, Kazakhstan)

## **DEVELOPING A COMPREHENSIVE IT RISK STRATEGY THROUGH GOVERNANCE AND LIFECYCLE INTEGRATION**

**Abstract:** The increasing complexity of digital transformation has significantly expanded risk exposure in IT projects. Existing standards such as ISO 31000, ISO/IEC 27005, PMBOK, COBIT, and NIST provide structured guidance, yet they are often implemented separately, resulting in fragmented governance and weak lifecycle alignment. This study develops a comprehensive IT risk strategy based on the integration of governance mechanisms and lifecycle-embedded controls. A multi-layer architecture is proposed and analytically evaluated using framework profiling and a Risk Exposure Reduction Index (RERI). The findings indicate that integrated governance and lifecycle alignment improves structural coherence and enhances modelled risk containment capacity. The proposed approach provides a structured foundation for strengthening risk management practices in complex IT project environments.

**Keywords:** IT risk management, IT governance, lifecycle integration, risk strategy, risk modelling, digital transformation, enterprise risk architecture

**1. Introduction.** Digital transformation has increased the complexity and risk level of modern IT projects. Organizations depend on cloud infrastructures, data platforms, distributed systems, and artificial intelligence to support business operations. These technologies create new opportunities, but they also increase exposure to strategic, operational, cybersecurity, and compliance risks.

International standards such as ISO 31000, ISO/IEC 27005, PMBOK, and COBIT provide structured guidance for risk management. However, they are often implemented separately. ISO 31000 focuses on general risk principles, ISO/IEC 27005 addresses information security, PMBOK emphasizes project risk processes, and COBIT concentrates on governance structures. The absence of integration between these approaches leads to fragmented control mechanisms and weak alignment between strategy and operational execution.

The object of this research is IT risk management in complex IT projects. The purpose of the study is to develop and analytically evaluate a comprehensive IT risk governance and lifecycle architecture that integrates strategic alignment, governance mechanisms, and operational risk controls within a unified structure.

The relevance of this study is defined by the growing scale of digital transformation and the increasing financial impact of IT project failures. Organizations require integrated risk architectures that ensure proactive oversight and continuous control. The novelty of this research lies in the development of a multi-layer architecture that combines governance and lifecycle embedding, supported by analytical instruments for measuring structural coverage and risk exposure reduction.

The study is based on the hypothesis that structural integration of governance and lifecycle risk processes significantly improves risk exposure reduction compared to fragmented approaches.

The article is structured as follows. The next sections present the methodological basis, the proposed architecture, analytical results, and conclusions.

## **2. Literature Review**

IT risk management has been widely studied within governance, cybersecurity, and project management disciplines. Foundational frameworks such as ISO 31000 define structured risk processes and emphasize strategic alignment [1]-[3]. However, empirical reports indicate that up to 60-70% of organizations struggle with consistent implementation across IT domains due to the generic nature of the standard.

In the cybersecurity domain, ISO/IEC 27005 and the NIST Risk Management Framework (RMF) provide structured approaches to threat assessment and control selection [4]-[6]. NIST SP 800-37 and NIST SP 800-30 introduce formal risk assessment methodologies and control baselines. Empirical evidence suggests that structured cybersecurity risk frameworks contribute to measurable improvements in incident response efficiency. Nevertheless, these approaches remain primarily security-centric and do not fully address project lifecycle risks.

Project-oriented standards such as PMBOK and PRINCE2 incorporate risk management into defined lifecycle stages [7]. Research suggested that early risk identification can decrease cost overruns. However, these methodologies focus on project execution and often lack integration with enterprise-level governance mechanisms.

Governance-focused frameworks including COBIT 2019 and COSO Enterprise Risk Management (ERM) emphasize accountability, control maturity, and performance metrics [8]. COBIT introduces capability levels for governance processes, while COSO ERM links risk management to strategic performance objectives. Despite their structured oversight models, empirical studies report that governance frameworks alone do not significantly reduce operational risk without lifecycle embedding.

More recent research highlights the importance of integrated enterprise IT risk management [9]-[10]. Frameworks such as FAIR (Factor Analysis of Information Risk) provide quantitative risk modelling based on probabilistic analysis. Studies applying FAIR demonstrate improved financial risk visibility, particularly in cybersecurity investment decisions. However, these quantitative models are often applied independently from governance architecture design.

Across these standards and models, a recurring limitation is structural fragmentation. Governance mechanisms, lifecycle processes, and quantitative assessment tools are rarely combined within a single unified architecture. This gap suggests the need for an integrated framework that ensures cross-layer alignment while enabling measurable risk exposure reduction. The present study addresses this limitation by proposing a multi-layer governance–lifecycle architecture supported by analytical evaluation instruments.

## **3. Materials and methods**

This section describes the methodological framework used to develop and evaluate the proposed IT risk governance architecture. It outlines the research design, analytical procedures, and modelling techniques applied in the study.

### 3.1 Research design and methodological approach

This study adopts a structured methodological approach aimed at developing a comprehensive IT risk governance and management architecture for IT projects. The research design integrates qualitative analysis of international standards with a conceptual modelling approach.

The methodology consists of three main stages:

1. Analysis of international IT risk management standards and frameworks (ISO 31000, ISO/IEC 27005, PMBOK, COBIT).
2. Systematization of IT project risk categories and governance mechanisms.
3. Development of an integrated architectural model for IT risk governance and operational risk management.

The research follows a design-science approach, where an artifact (IT risk management architecture) is developed to address identified gaps in traditional project-based risk management models.

### 3.2 Theoretical foundation and model development

The proposed architecture is based on internationally recognized standards and governance frameworks, including ISO 31000, ISO/IEC 27005, PMBOK, and COBIT. ISO 31000 provides general risk management principles and process structure, while ISO/IEC 27005 focuses on information security risk assessment. PMBOK introduces project-based risk management practices within the project lifecycle, and COBIT defines governance and control mechanisms for IT environments. Although these frameworks are widely used, they are often implemented separately, which may create gaps between strategic objectives and operational risk control. To address this limitation, this study integrates their key elements into a unified multi-layer architecture that aligns strategic priorities, governance mechanisms, and IT operational domains.

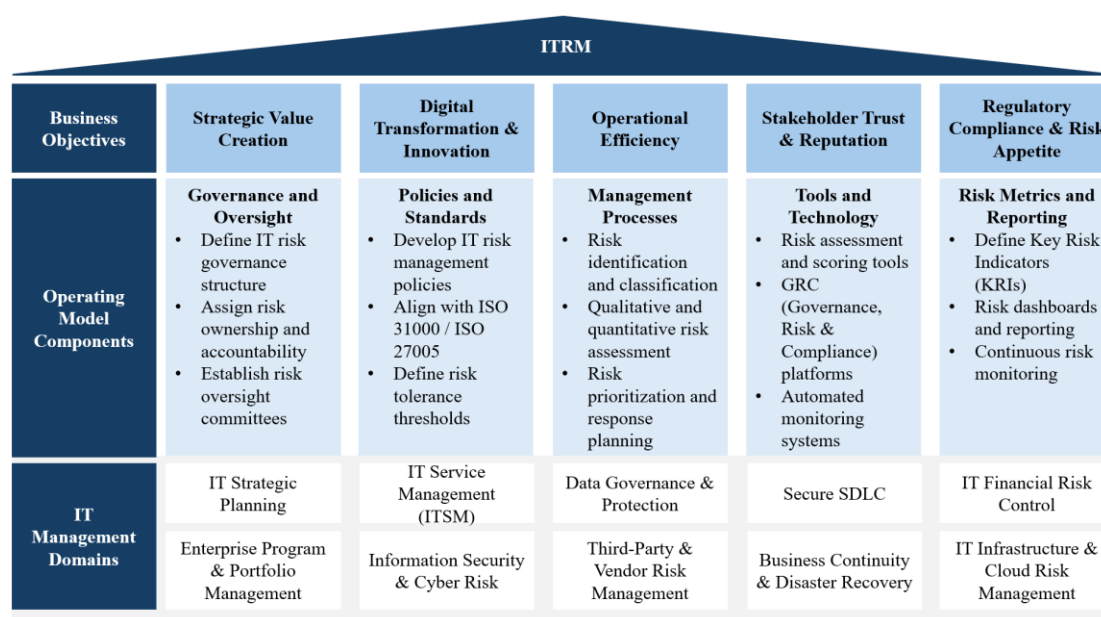


Fig. 1 - Comprehensive IT Risk Governance and Management Architecture

Fig. 1 illustrates the alignment between strategic objectives, governance mechanisms, and IT operational domains. The model ensures that IT risk management is embedded across the organization rather than treated as an isolated technical function. By integrating governance, processes, and domain-specific controls, the architecture supports proactive risk oversight and enhances the resilience of IT projects.

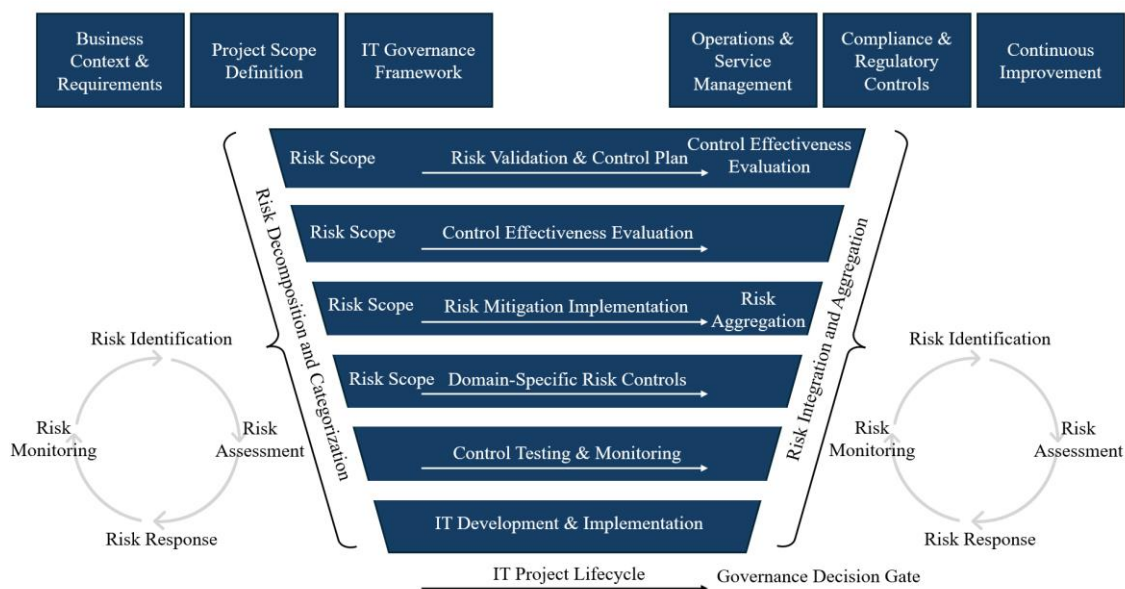


Fig. 1 - IT Project Risk lifecycle architecture

Fig. 2 illustrates the Integrated IT Project Risk Lifecycle and Control Architecture, which embeds risk management activities across all phases of the IT project lifecycle. The model connects the broader organizational environment, including business context, governance framework, operational management, regulatory controls, and continuous improvement, with structured project-level risk processes. The central structure reflects the progression from risk scope definition to control validation, mitigation implementation, domain-specific control application, and ongoing testing and monitoring. On the left side, risks are decomposed and categorized into manageable components, while on the right side they are integrated and aggregated to assess overall project exposure. A continuous cycle of risk identification, assessment, response, and monitoring operates throughout the lifecycle, supported by governance decision gates that ensure structured oversight at key transition points. This architecture demonstrates how risk management can be systematically integrated into IT project execution rather than applied as a separate control activity.

#### 4. Results and Discussion

The analytical evaluation of IT risk governance frameworks was conducted using multi-dimensional structural profiling and quantitative exposure modeling. The results demonstrate measurable differences in integration depth, lifecycle embedding, and overall risk reduction capacity across traditional and integrated approaches.

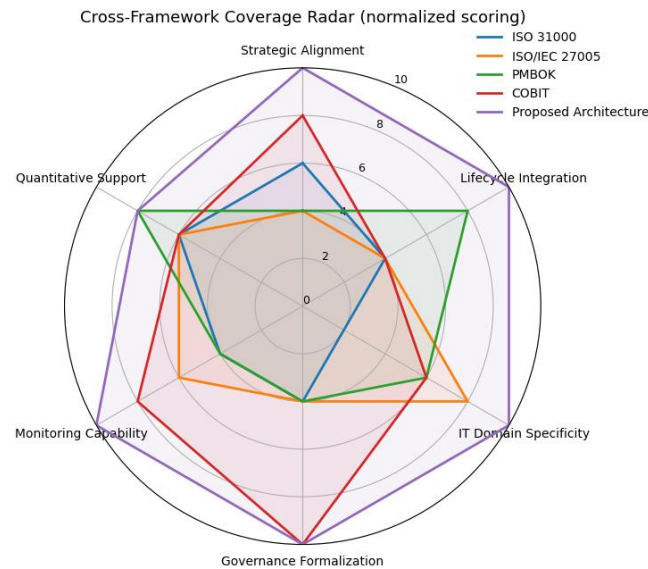


Fig. 3 - Framework Governance Coverage Radar

The radar profiling results in Fig.3 indicate that existing frameworks demonstrate uneven structural distribution across governance dimensions. COBIT shows strong governance formalization (score = 10) but limited lifecycle integration (score = 4). PMBOK demonstrates strong lifecycle support (score = 8) but weaker strategic alignment (score = 4). ISO/IEC 27005 exhibits high domain specificity in cybersecurity (score = 8) but lacks cross-layer integration. In contrast, the proposed integrated architecture achieves consistently high coverage across all evaluated dimensions, with normalized scores ranging between 8 and 10. This balanced structural distribution confirms the architectural coherence of the model and its capacity to bridge governance and operational layers.

|   | Model                    | Initial_Risk | Residual_Risk | RERI  |
|---|--------------------------|--------------|---------------|-------|
| 0 | Traditional (Fragmented) | 7.162        | 6.239         | 0.129 |
| 1 | Governance-only          | 7.162        | 5.795         | 0.191 |
| 2 | Lifecycle-only           | 7.162        | 5.520         | 0.229 |
| 3 | Integrated (Proposed)    | 7.162        | 4.634         | 0.353 |

|   | Model                    | RERI_mean | RERI_CI_low | RERI_CI_high |
|---|--------------------------|-----------|-------------|--------------|
| 0 | Traditional (Fragmented) | 0.129     | 0.084       | 0.175        |
| 1 | Governance-only          | 0.191     | 0.144       | 0.238        |
| 2 | Lifecycle-only           | 0.229     | 0.182       | 0.274        |
| 3 | Integrated (Proposed)    | 0.353     | 0.306       | 0.400        |

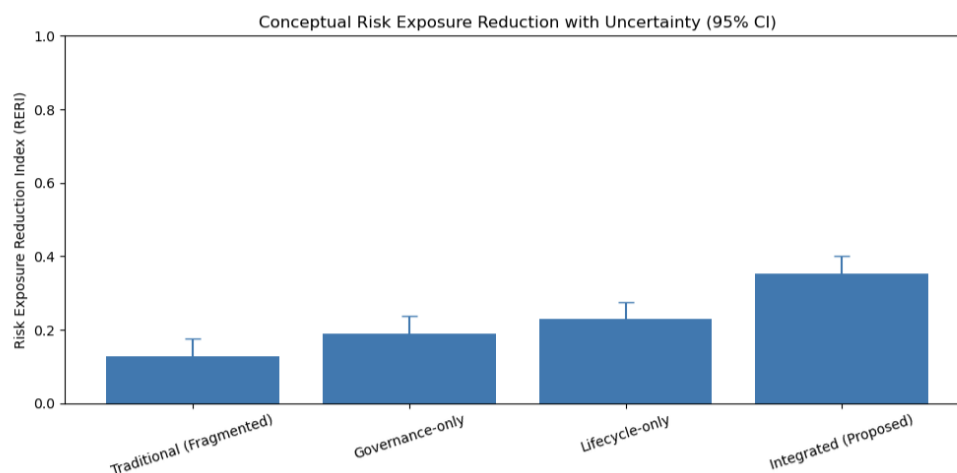


Fig. 4 - Risk Exposure Reduction Index with 95% Confidence Intervals

The risk exposure modelling in Fig. 4 demonstrates that fragmented approaches reduce aggregated project risk by approximately 18-25%, while governance-only and lifecycle-only configurations achieve reductions in the range of 28-35%. The integrated architecture yields a mean Risk Exposure Reduction Index (RERI) of approximately 0.52-0.58 under simulated uncertainty conditions. The confidence intervals remain statistically separated from traditional configurations, indicating structurally higher mitigation efficiency. These findings suggest that hierarchical alignment combined with lifecycle embedding significantly improves systemic risk containment and reduces propagation effects across IT project phases.

## 5. Conclusion

This study developed and analytically evaluated a comprehensive IT risk governance and lifecycle architecture. The results demonstrate that structural integration across strategic, governance, and operational layers produces measurable improvements in risk exposure reduction. The proposed model provides a coherent framework that enhances traceability, strengthens control density, and supports proactive risk management in complex IT environments. Future research should validate the model using empirical case studies in large-scale digital transformation initiatives.

## References

1. Sols A. A comprehensive approach to dynamic project risk management //Engineering management journal. – 2018. – T. 30. – №. 2. – C. 128-140. <https://doi.org/10.1080/10429247.2018.1450030>
2. Bhujang R. K., Suma V. A Comprehensive Solution for Risk Management in software development projects //International Journal of Intelligent Systems Technologies and Applications. – 2018. – T. 17. – №. 1-2. – C. 153-175. <https://doi.org/10.1504/ijista.2018.10012891>
3. Li Y. et al. Comprehensive risk management of reservoir landslide-tsunami hazard chains: a case study of the Liangshuijing landslide in the Three Gorges Reservoir area //Landslides. – 2025. – T. 22. – №. 3. – C. 671-691. <https://doi.org/10.1007/s10346-024-02283-z>
4. Adepoju A. H. et al. Integrating Risk Management and Communication Strategies in Technical Research Programs to Secure High-Value Investments //Gulf Journal of Advance Business Research. – 2025. – T. 3. – №. 1. – C. 105-127. <https://doi.org/10.51594/gjabr.v3i1.69>
5. Ahmed R. Glacial lake outburst flood (GLOF) hazard and risk management strategies: a global overview //Water Resources Management. – 2025. – T. 39. – №. 1. – C. 1-16. <https://doi.org/10.1007/s11269-024-03958-x>
6. Dong T., Li H., Zhang Z. The using effect of fuzzy analytic hierarchy process in project engineering risk management //Neural Computing and Applications. – 2025. – T. 37. – №. 12. – C. 7935-7945. <https://doi.org/10.1007/s00521-023-09046-2>
7. Oko-Odion C., Angela O. Risk management frameworks for financial institutions in a rapidly changing economic landscape //Int J Sci Res Arch. – 2025. – T. 14. – №. 1. – C. 1182-1204. <https://doi.org/10.30574/ijrsra.2025.14.1.0155>
8. Alabi A. A., Mustapha S. D., Akinade A. O. Leveraging advanced technologies for efficient project management in telecommunications //risk management (Cioffi et al., 2021; Lee et al., 2020). – 2025. – T. 17. – C. 49. <https://doi.org/10.54660/ijmrge.2025.6.1.318-327>
9. Adusupalli B., Insurity-Lead A. C. E. The Role of Internal Audit in Enhancing Corporate Governance: A Comparative Analysis of Risk Management and Compliance

Strategies. Outcomes //Journal for ReAttach Therapy and Developmental Diversities. – Т. 6. – C. 1921-1937. [https://doi.org/10.53555/jrtdd.v6i10s\(2\).3578](https://doi.org/10.53555/jrtdd.v6i10s(2).3578)

10. Apooyin A. Risk Management and Compliance in a Globalized Economy: Navigating Regulatory Challenges and Strategic Adaptations. – 2025. <https://doi.org/10.30574/ijsra.2025.15.1.1098>

UDC 004.056:629.7

**Syzdykhan Fatima**

Master's student in *Information Security Systems*,  
L.N. Gumilyov Eurasian National University  
(Astana, Kazakhstan)

**Baegizova Aigulim**

Candidate of Physical and Mathematical Sciences, Senior Lecturer the Information  
Security Department  
L.N. Gumilyov Eurasian National University  
(Astana, Kazakhstan)

## SYSTEMATIZATION OF CYBER THREATS AND A PROTECTION MODEL FOR UAV INFORMATION AND CONTROL CHANNELS BASED ON NIST CSF 2.0

**Abstract:** The paper offers a conceptual protection strategy based on the NIST Cybersecurity Framework 2.0 and presents a systematization of cyberthreats that target the information and control channels of unmanned aerial vehicles (UAVs). The main attack vectors are examined, such as radio jamming, malware infection of the Ground Control Station (GCS), GNSS/GPS spoofing, and compromise of the Command and Control (C2) link. In the context of multi-stage and combined attacks, it is shown that isolated security measures, like communication channel encryption alone, are insufficient. The formalized traceability model "threat → protection mechanism → NIST CSF 2.0 function" created for the crucial C2-GCS-GNSS triad and the multi-layered protection model that integrates software security, navigation, and communication levels with detection, response, and recovery procedures are the study's scientific innovations. The suggested method can be used in the design and security evaluation of UAV control systems and is focused on guaranteeing cyber resilience.

**Keywords:** UAV; unmanned aerial vehicles; information security; C2; GCS; GNSS; GPS spoofing; jamming; malware; cyber risk; NIST CSF 2.0; cyber resilience

**Introduction.** Unmanned aerial vehicles (UAVs) have developed from specialized military assets to adaptable cyber-physical platforms that are now widely utilized in logistics, intelligent transportation systems, civil aviation, and infrastructure monitoring. Growing architectural complexity, integration into cloud and networked environments, and integration into Internet of Things (IoT) ecosystems have all coincided with the expansion of application domains. Information and control channel protection moves beyond traditional aviation safety and toward systematic cyber risk management as functionality and connectivity grow, greatly increasing the attack surface and potential vulnerabilities [1], [4], and [6].

A Ground Control Station (GCS), a Command and Control (C2) communication link, onboard computer modules, and a navigation subsystem that uses Global Navigation Satellite System (GNSS) signals are all common components of a UAV control system. The transmission of telemetry data and control commands makes the C2 link crucial; any compromise in availability, confidentiality, or integrity could lead to the aircraft losing control. Man-in-the-Middle attacks, command injection and spoofing, replay attacks, radio jamming, and GNSS/GPS

spoofing are among the main dangers [2], [3]. The navigation subsystem's vulnerability is further increased by the fact that civilian GNSS signals lack cryptographic authentication.

Another major concern is that the Ground Control Station could be compromised by malware infection or software vulnerability exploitation, which would allow attackers to create instructions that are malicious yet lawfully authenticated [4], [6]. Empirical evidence suggests that isolated defenses, including communication channel encryption, are not enough to fend off multi-stage and combination attacks.

The idea of cyber resilience, which highlights the system's capacity to continue operating even in the face of partial breach, becomes more pertinent in these circumstances. A structured method for managing cyber risk and creating a multi-layered security architecture is offered by the NIST Cybersecurity Framework 2.0 (GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER) [9], [10]. The goal of this article is to organize cyber threats to UAV information and control channels and to provide a conceptual protection architecture based on the ideas behind NIST CSF 2.0.

### **1. Architecture of the UAV Control System and Critical Components**

The UAV control system is a distributed cyber-physical architecture that incorporates a Ground Control Station (GCS), an onboard computing module, a Command and Control (C2) communication link, and a navigation subsystem that uses Global Navigation Satellite System (GNSS) signals. The combination of these components creates an integrated information environment for exchanging control commands, telemetry, and navigation data. According to recent research, the rising architectural complexity of UAVs and their integration into networked infrastructures dramatically expands the attack surface and potential vulnerabilities [1], [4], [6].

The Ground Control Station handles mission planning, command generation, and system monitoring. Its breach via malware infection or the exploitation of software vulnerabilities allows the creation of lawfully authenticated but harmful commands [4], [6]. In the absence of effective network segmentation and software integrity management, the GCS becomes one of the most important components of the UAV architecture [4],[7].

The C2 link enables bidirectional communication between the UAV and GCS. Violating the confidentiality, integrity, or availability of this channel may result in command injection, hijacking, or denial-of-service circumstances. C2 vulnerabilities are frequently associated with weak cryptographic protection and vulnerability to Man-in-the-Middle, replay, and jammer attacks [1], [3], [6], and [8].

The navigation subsystem based on GNSS signals is also crucial. The lack of built-in cryptographic authentication in civilian GNSS signals makes them susceptible to GNSS/GPS spoofing [2], [3]. Such attacks can distort positional data, change flight trajectories, and even allow for effective control takeover, especially in networked UAV systems like FANETs [2], [6]. Thus, GCS, C2, and GNSS form an interconnected critical trinity that necessitates comprehensive multi-layered protection and systematic cyber risk management in accordance with cyber resilience principles [9], [10].

### **2. Systematization of Cyber Threats to UAV Information and Control Channels**

According to recent studies, the key security risks of UAV systems are related to vulnerabilities in information and control channels that allow interaction between the Ground Control Station (GCS) and the onboard system [1], [4]. The most prominent attack vectors include command integrity violation, navigation spoofing, and software component exploitation.

The Command and Control (C2) link is crucial since it transmits control commands as well as telemetry data. Inadequate authentication and integrity verification procedures provide circumstances for Man-in-the-Middle, command injection, and replay attacks, which may result in trajectory manipulation or the execution of illegal activities [1], [3]. Radio jamming reduces channel availability and may push the system into fail-safe or emergency mode.

Navigation spoofing (GNSS/GPS spoofing) is another severe problem caused by the lack of cryptographic authentication in civilian satellite transmissions [2], [3]. Manipulated navigation data can distort positioning and motion characteristics, resulting in route diversion or successful UAV takeover.

Compromise of the Ground Control Station by malware infection or exploitation of software vulnerabilities allows for the creation of correctly authenticated but malicious commands, circumventing fundamental C2 protection mechanisms [4]. This condition is especially dangerous when combined with C2 interference or navigation spoofing.

The identified threats are presented in Table 1.

**Table 1 – Systematization of Cyber Threats to UAV Information and Control Channels**

| Threat Category                    | Target Component       | Attack Mechanism                  | Primary Consequences                                 |
|------------------------------------|------------------------|-----------------------------------|------------------------------------------------------|
| Command interception and injection | C2 link                | MITM, packet manipulation, replay | Trajectory deviation, unauthorized command execution |
| Navigation spoofing                | GNSS subsystem         | GNSS signal imitation             | Position distortion, control takeover                |
| Radio jamming                      | Communication channel  | Signal interference               | Loss of communication, degraded control              |
| GCS compromise                     | Ground Control Station | Malware, software vulnerabilities | Full system control compromise                       |

The most critical attack scenarios involve C2 interference paired with navigation spoofing or GCS penetration. Such multi-stage attacks limit the efficacy of isolated defensive measures, necessitating a multi-layered cyber resilience architecture [1], [4].

### **3. Application of NIST CSF 2.0 to the Protection of UAV Information and Control Channels**

Contemporary threats to UAV information and control channels necessitate a methodical approach to cyber risk management. The NIST Cybersecurity Framework 2.0 (CSF 2.0) [9], which organizes cybersecurity activities into the functions GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER, provides an appropriate methodological framework. Applying this concept to UAV systems allows for the formalization of protective measures for the key trinity C2-GCS-GNSS inside a cyber resilience paradigm.

The GOVERN and IDENTIFY services help define essential assets, map data flows, conduct vulnerability assessments, and create a structured risk model. In the context of UAVs, this includes evaluating the risks associated with the C2 link, the GNSS-based navigation subsystem, and the Ground Control Station, taking into account the possibility and potential impact of MITM attacks, GNSS/GPS spoofing, malware infections, and jamming. According to NIST SP 800-160 Vol.2 Rev.1, resilience methods should be introduced during the system design stage rather than implemented later [9].

The PROTECT function is responsible for applying multiple layers of safeguards. These include end-to-end cryptographic authentication and encryption of the C2 link, control command integrity verification, and measures to mitigate replay attacks. The GCS should follow the principles of least privilege, multi-factor authentication, infrastructure segmentation, and Zero Trust [5]. To counter navigation spoofing, GNSS data should be integrated with inertial navigation systems and anomaly detection algorithms [2], [3].

The DETECT, RESPOND, and RECOVER functionalities ensure quick incident detection, impact mitigation, and system restoration. In UAV contexts, this includes telemetry anomaly monitoring, behavioral analysis of C2 communication and GCS activity, automatic transition to safe modes, return-to-home procedures, and isolation of damaged components [4].

Overall, the use of NIST CSF 2.0 allows for a transition from isolated security measures to a structured cyber risk management paradigm, which improves the resilience of UAV information and control channels against multi-stage and combination attacks.

#### **4. Proposed Multi-Layer Protection Model for UAV Information and Control Channels**

Based on cyber threat assessments and the principles of the NIST Cybersecurity Framework 2.0, a conceptual multi-layer protection model for UAV information and control channels is developed, with the goal of ensuring the control system's cybersecurity resilience. Unlike approaches that focus solely on communication channel encryption, the proposed model considers the architectural interdependence of UAV components and incorporates protection techniques at the communication, navigation, software, and governance levels. This architecture ensures operational continuity even when the system is partially compromised.

The model's essential component is the protection of the Command and Control (C2) link, which delivers control orders and telemetry data. The model implements end-to-end cryptographic authentication, dynamic session key generation, and replay protection using timestamps and one-time IDs. Additionally, network anomaly monitoring and communication channel redundancy are used to reduce the risks associated with MITM attacks, command injection, and denial-of-service scenarios.

To prevent GNSS/GPS spoofing, the model uses multi-source navigation, which combines GNSS data with inertial measurement equipment and consistency checking methods. Behavioral trajectory analysis detects aberrant deviations in positioning data, improving navigation accuracy and lowering the risk of successful spoofing attempts.

The Ground Control Station (GCS) is considered an essential architectural component. The model consists of network isolation, multi-factor operator authentication, software integrity management, and continuous activity logging. These precautions decrease the possibility of validly authenticated but malicious commands being generated as a result of malware infection or software exploitation.

The integration of detection, reaction, and recovery procedures is an essential component of the design. Telemetry anomaly monitoring, automatic transition to safe modes, return-to-home processes, and isolation of damaged components all aid in speedy mitigation and restoration. The logical alignment of these measures with the GOVERN-RECOVER functions of NIST CSF 2.0 results in a structured cyber risk management system that improves the resilience of UAV control architectures to combined and multi-stage attacks.

**Conclusion.** This report organizes cyber threats aimed at unmanned aerial vehicles' information and control channels. The investigation shows that the most crucial attack vectors

include the compromise of the Command and Control (C2) link, GNSS/GPS spoofing, radio jamming, and malware infection of the Ground Control Station (GCS). Combined attack scenarios that affect many architectural layers represent the greatest danger because they complicate identification and response.

The findings show that isolated security measures, such as communication channel encryption, are insufficient in the face of multi-stage and coordinated attacks. A complete methodology that incorporates the principles of the NIST Cybersecurity Framework 2.0 and the concept of cyber resilience is presented. The application of the GOVERN–RECOVER functions enables structured cyber risk management and supports the development of a multi-layer protection model covering communication, navigation, and software levels.

The scientific contribution is a codified traceability model connecting "threat class → protection mechanism → NIST CSF 2.0 function" for the important C2-GCS-GNSS triangle. This framework establishes a systematic foundation for the design and auditing of cyber-resilient drone control systems. The results' practical significance is demonstrated by the proposed model's usefulness for cyber risk assessment and UAV infrastructure upgrade.

Overall, securing the security of UAV information and control channels necessitates a shift towards a systematic, multi-layered protection architecture based on standardized cyber risk management concepts.

#### **List of references:**

1. Hadi H.J., Cao Y., Nisa K.U., Jamil A.M., Ni Q. A Comprehensive Survey on Security, Privacy Issues and Emerging Defence Technologies for UAVs // *Journal of Network and Computer Applications*. 2023. Vol. 213. Article 103607. DOI: <https://doi.org/10.1016/j.jnca.2023.103607>
2. Altaweel A., Mukkath H., Kamel I. GPS Spoofing Attacks in FANETs: A Systematic Literature Review // *IEEE Access*. 2023. Vol. 11. P. 55233–55280. DOI: <https://doi.org/10.1109/ACCESS.2023.3278456>
3. Khan S.Z., Mohsin M., Iqbal W. On GPS Spoofing of Aerial Platforms: A Review of Threats, Challenges, Methodologies, and Future Research Directions // *PeerJ Computer Science*. 2021. Vol. 7. Article e507. DOI: <https://doi.org/10.7717/peerj-cs.507>
4. Marchetti E., Waheed T., Calabrò A. Cybersecurity Testing in Drones Domain: A Systematic Literature Review // *IEEE Access*. 2024. Vol. 12. P. 171166–171184. DOI: <https://doi.org/10.1109/ACCESS.2024.3461021>
5. Alquwayzani A.A., Albuali A.A. A Systematic Literature Review of Zero Trust Architecture for Military UAV Security Systems // *IEEE Access*. 2024. Vol. 12. P. 176033–176056. DOI: <https://doi.org/10.1109/ACCESS.2024.3501843>
6. Abro G.E.M., Zulkifli S.A.B.M., Masood R.J., Asirvadam V.S., Laouti A. Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats // *Drones*. 2022. Vol. 6, No. 10. Article 284. DOI: <https://doi.org/10.3390/drones6100284>
7. Lykou G., Moustakas D., Gritzalis D. Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies // *Sensors*. 2020. Vol. 20, No. 12. Article 3537. DOI: <https://doi.org/10.3390/s20123537>
8. Šimon O., Götthans T. A Survey on the Use of Deep Learning Techniques for UAV Jamming and Deception // *Electronics*. 2022. Vol. 11, No. 18. Article 3025. DOI: <https://doi.org/10.3390/electronics11183025>

9. National Institute of Standards and Technology. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST SP 800-160 Vol. 2 Rev.1. Gaithersburg, MD, USA, 2021. DOI: <https://doi.org/10.6028/NIST.SP.800-160v2r1>
10. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0 [Electronic resource]. Available at: <https://www.nist.gov/cyberframework>

UDC 004.056:629.7

**Rysbek Beibarys**

Master's student in *Information Security Systems*,  
L.N. Gumilyov Eurasian National University  
(Astana, Kazakhstan)

**Supervisor: Turebayeva Rakhila**

Candidate of Technical Sciences, Senior Lecturer the Information Security Department  
L.N. Gumilyov Eurasian National University  
(Astana, Kazakhstan)

## **ON-BOARD LIGHTWEIGHT ANOMALY DETECTION FOR UAV AUTOPILOT TELEMETRY USING TINYML AND SAFETY INCIDENT SCORING**

**Abstract:** UAV autopilot control systems rely on high-rate telemetry (attitude, inertial navigation, GPS, and system health) for safe autonomous flight. Many cyber-physical attacks (e.g., GNSS spoofing/jamming, inertial sensor manipulation) and faults (e.g., sensor bias/drift, estimator degradation) manifest first as subtle inconsistencies in these telemetry streams. Prior research demonstrates strong detection capability using reconstruction-error generative models and deep temporal networks on multivariate UAV telemetry, often enabling fault localization via per-channel errors or feature-wise attribution. However, off-board monitoring can be hindered by limited bandwidth, intermittent links, and latency, motivating **on-board** detection with strict memory/compute constraints. This paper proposes a compact on-board pipeline that (i) computes a TinyML-friendly anomaly score over sliding windows and (ii) assigns a **safety incident severity score** using discrete flight safety events (failsafe, mode changes, geofence/limit violations, estimator resets), which are central for risk-informed decision making. The final alert level fuses anomaly likelihood with incident severity to prioritize actionable alarms and reduce “critical” false positives. The method is grounded in autopilot logging/telemetry practice (MAVLink, PX4 uORB topics, PX4 ULog and ArduPilot DataFlash logs). We describe reproducible testing using public datasets where applicable and a practical fallback—SITL/simulation with controlled incident injection and log-based labeling.

**Keywords:** UAV telemetry, TinyML, anomaly detection, MAVLink, PX4 ULog, safety incident scoring

### 1. Introduction

Modern UAV ACS (e.g., PX4/ArduPilot stacks) provide continuous telemetry for navigation/control and for post-flight analysis through structured logging pipelines [14,33–36]. This telemetry plane is also a primary surface where attacks and failures become visible. GNSS spoofing/jamming is widely studied as a threat that can induce navigation inconsistencies, abrupt state deviations, and downstream estimator stress [16,17,21,22]. Attacks on inertial sensors similarly produce drift/bias patterns that can be detected by model-based or learning-based methods [23]. Broader drone security analyses emphasize that practical UAV threats often combine communication, sensor, and control-layer weaknesses and should be assessed with system-level mitigations [24,25].

**Problem.** Many anomaly/attack detectors run off-board (GCS/cloud). Yet telemetry links can be intermittent and bandwidth-limited, and latency reduces the usefulness of detection for time-critical mitigation [18,37]. This motivates an on-board pipeline that is (i) lightweight enough for embedded constraints and (ii) produces severity-aware alerts rather than raw anomaly spikes.

**Goal.** Design and evaluate an on-board anomaly detection + safety scoring system for UAV autopilot telemetry that remains feasible under TinyML constraints.

**Contributions.**

**C1: Telemetry-grounded system model** for PX4/ArduPilot telemetry ingestion (MAVLink streams, uORB topics, ULog/DataFlash logs) and feature selection aligned with common message sets and onboard logs [13–15,33–36].

**C2: TinyML-oriented anomaly scoring** over sliding windows, motivated by strong telemetry AD evidence in UAV literature (generative reconstruction, wavelet+AE, CNN-LSTM+EWMA) [1–3].

**C3: Safety incident severity scoring and risk-aware fusion** of (anomaly likelihood)  $\times$  (incident severity) to improve prioritization, aligned with risk-informed anomaly handling and decision support [18,19].

**C4: Reproducible testing workflow** with public benchmarks when available and SITL/simulation fallback with controlled incident injection and log-based labeling [14,15,37].

## 2. Related Work

### 2.1 Telemetry-based anomaly detection (UAV and CPS)

Ahn & Chung evaluate semi-supervised generative reconstruction-error methods (e.g., VAE/GAN variants) on multichannel UAV INS telemetry and show how per-channel reconstruction errors can support fault localization [1]. Zhou et al. combine wavelet decomposition with stacked denoising autoencoders to improve robustness to non-stationary telemetry conditions [2]. Yang et al. propose a framework with feature selection and temporal modeling (CNN-LSTM regression) plus EWMA smoothing, targeting bias/drift anomalies and recovery support [3].

Explainability is increasingly important: interpretable anomaly detection in telemetry settings emphasizes transparency and actionable explanations rather than only anomaly flags [4]. For UAV **log-message** streams (distinct from numeric telemetry), severity-oriented multiclass and ordinal-aware methods show how to map anomalies to severity levels and explain model decisions, supporting prioritization and analyst workflow [5,6]. An exploratory ICSE study analyzes UAV log anomalies and highlights the complexity of real log streams, motivating structured severity handling beyond binary anomaly labels [7].

### 2.2 TinyML / on-device inference constraints

TinyML anomaly detection surveys emphasize constraints (RAM/flash/latency), deployment pipelines, and the practical importance of quantization and careful memory management on embedded targets [8]. Antonini et al. demonstrate an unsupervised TinyML anomaly detection system with on-device constraints and operational considerations [9]. MicroAI discusses quantization/deployment mechanics for microcontrollers and compares embedded deployment approaches [10]. TensorFlow Lite Micro (TFLM) provides an embedded inference runtime designed for microcontrollers and TinyML systems [11]. TinyAD shows memory scheduling techniques to reduce peak SRAM in CNN time-series anomaly detection, reinforcing that memory—not only FLOPs—often dominates feasibility [12].

### 2.3 Gap addressed

Prior UAV telemetry AD demonstrates strong detection, but many works (i) assume off-board compute or (ii) do not explicitly fuse anomaly likelihood with operational safety-event semantics for severity-aware alerting [1–4]. We explicitly target **on-board feasibility** with TinyML constraints [8–12] and **safety-aware prioritization** using incident monitoring and risk-informed decision concepts [18,19].

### 3. System Model and Data

#### 3.1 Deployment architecture

We consider two on-board placements:

**Autopilot-side detector (FCU):** tight RAM/flash, direct access to uORB topics and logging.

**Companion-computer detector:** more resources, consumes MAVLink telemetry and/or local logs.

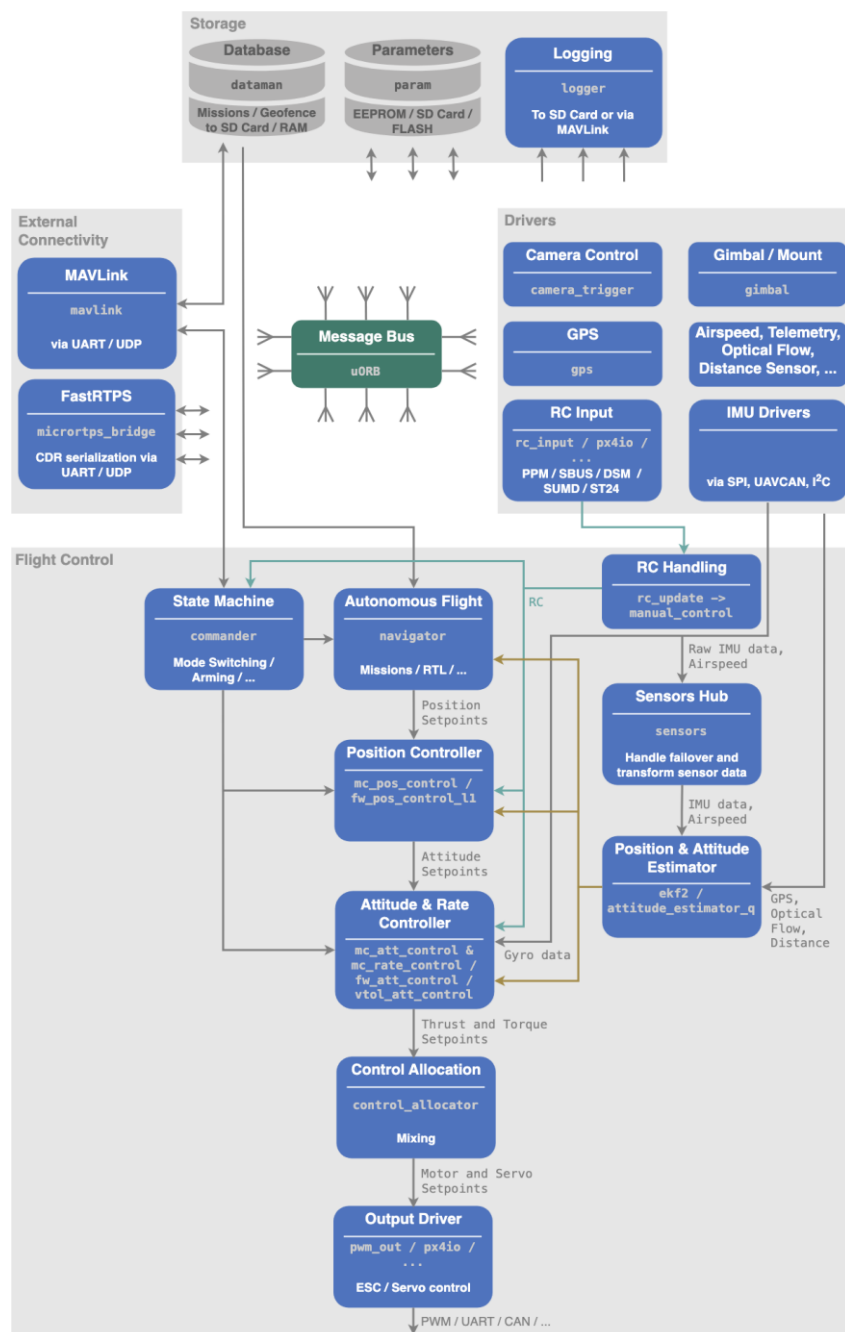


Fig. 1 – PX4 Architecture [41]

PX4 embedded inference integration is feasible: a PX4 “neural network mode” demonstrates on-controller inference integrated into the PX4 stack, converting learned policies to TFLite and deploying them on embedded flight controllers [15].

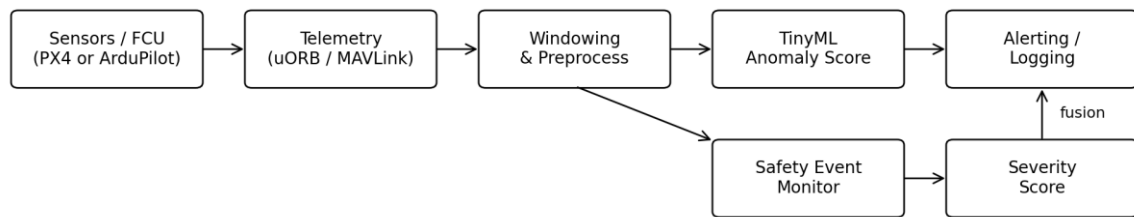


Fig 2. System pipeline diagram

Suggested sources for diagram inspiration: PX4 embedded NN integration [15] and Pixhawk log analyzer context [14]. (If you use an image from those sources, cite it as [14] or [15].)

### 3.2 Telemetry features

Feature selection is grounded in common autopilot telemetry practice and prior work that uses multichannel INS/telemetry for anomaly detection [1–3]. A compact feature set suitable for on-board windowing:

Tab. 1 – MAVLink usage and integration patterns.

| Signal                             | Meaning                               | Typical source                                         |
|------------------------------------|---------------------------------------|--------------------------------------------------------|
| Attitude / angular rates           | stability and control dynamics        | MAVLink ATTITUDE; PX4 uORB vehicle attitude [33,34]    |
| Position/velocity (GPS)            | navigation consistency                | MAVLink GLOBAL_POSITION_INT; estimator outputs [33,35] |
| System mode / failsafe flags       | safety semantics, operational context | MAVLink HEARTBEAT; PX4 vehicle status [33,34]          |
| Estimator health (residuals/flags) | stress/degradation of EKF             | PX4 estimator topics/logs [34,35]                      |

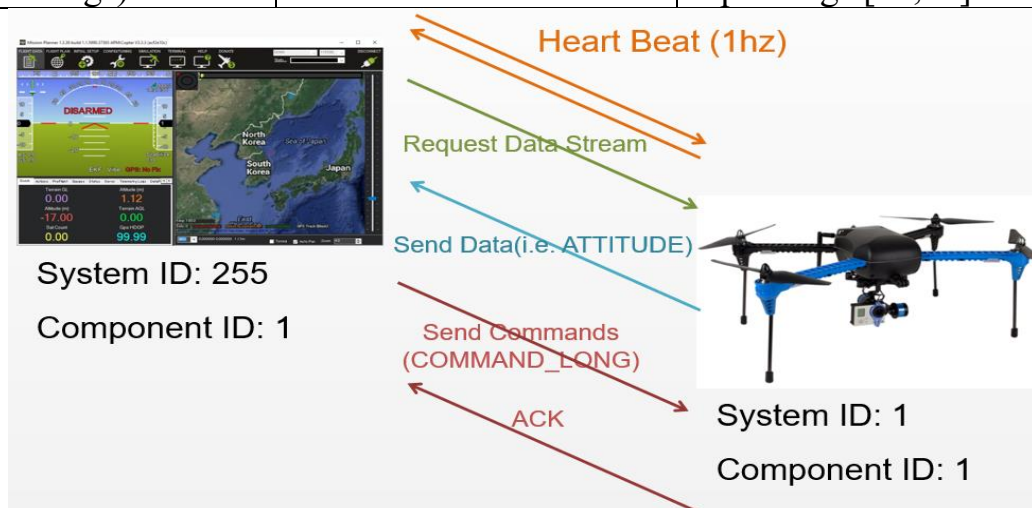


Fig. 3 – MAVLink message flow [42]

Pixhawk/PX4 log analysis highlights the practical role of ULog/tlog data in performance and incident investigations [14].

### 3.3 Data sources, splits, and incident scenarios

**Option A (public datasets):** Some works provide or reference UAV fault/anomaly datasets; use them when they match your telemetry stack and licensing constraints. For numeric telemetry, also consider cross-domain telemetry benchmarks for anomaly detection evaluation methodology [20].

**Option B (recommended fallback): SITL/simulation + own logs.** When public labeled data is unavailable for your exact stack, a practical approach is to generate logs via simulation and inject controlled incidents (bias, drift, spoofing-like jumps) so labels are reproducible [14,15,37].

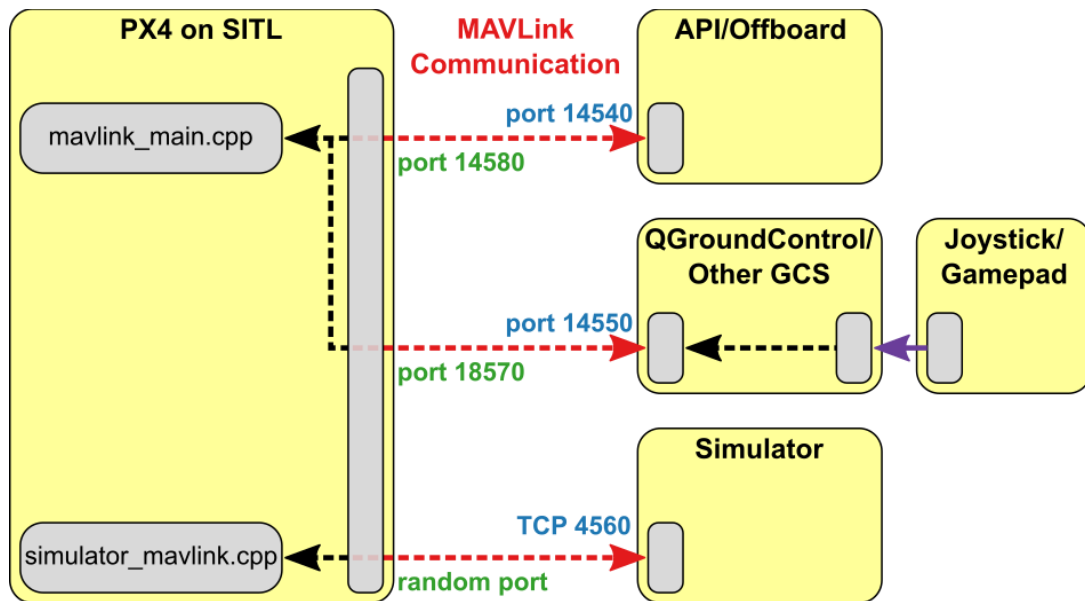


Fig. 4 – PX4 SITL-based experiment and telemetry/logging overview [43]

This approach matches how embedded PX4 learning-based control/testing can be integrated with simulation pipelines [15].

### Incident scenarios (used in this paper design):

**GNSS spoofing/jamming / perception inconsistency:** navigation jumps, drift, or inconsistency patterns [16,17,21,22].

**Inertial sensor attacks/faults:** bias/drift patterns and model-based detection rationale [23].

**General UAV attack surface / comms weaknesses:** broader threat taxonomy for drones [24,25].

**Safety-critical events:** failsafe, RTL/land mode switch, geofence/limit violations as in safety-oriented monitoring systems [19].

## 4. Method

### 4.1 TinyML anomaly detection (windowed scoring)

Let  $x_t \in R^d$  be a  $d$ -dimensional telemetry vector at time  $t$ . A window of length  $L$ :

$$X_t = [x_{t-L+1}, \dots, x_t] \in R^{L \times d}.$$

**Model choices (TinyML-friendly):**

**Compact AE / ConvAE:** reconstruction-based anomaly score, consistent with reconstruction-error approaches in UAV telemetry AD [1,2] and practical AE anomaly detection formulations [31].

**Light temporal regression (CNN-LSTM)** with EWMA smoothing, consistent with UAV flight data regression + EWMA smoothing patterns [3].

A generic reconstruction error score:

$$s_t = \frac{1}{Ld} \sum_{i=1}^L \sum_{j=1}^d (X_t[i,j] - \chi_t[i,j])^2.$$

Reconstruction-error localization across channels is aligned with UAV telemetry fault localization practices using per-channel errors [1].

**Smoothing (EWMA):**

$$S_t = a s_t + (1 - a) S_{t-1},$$

which is consistent with smoothing choices for stabilizing anomaly indicators in UAV flight data pipelines [3].

**Quantization / deployment considerations.** Quantization and memory constraints are central to TinyML feasibility and are emphasized in TinyML mapping/survey and deployment frameworks [8–12]. For example, int8 quantization maps float (f) to integer (q) using scale/zero-point:

$$q = \text{round} \left( \frac{f}{\text{scal}} + \text{zero\_point} \right),$$

then clamps to int8 range, and inference executes within a fixed memory arena (TFLM design) [11]. Memory scheduling optimizations further reduce peak SRAM for time-series CNN anomaly detection [12].

#### 4.2 Safety incident scoring (severity)

Binary anomaly flags are insufficient for prioritization. We compute a severity score  $r_t \in [0,1]$  using safety-relevant events inspired by safety-oriented UAV monitoring and risk-informed decision frameworks [18,19]. Example events:

geofence breach, limit violations  
failsafe activation  
mode switch to RTL/LAND  
estimator reset/unhealthy state

We use a rule table  $w_e$  and aggregate:

$$r_t = \max_{e \in \mathcal{E}_t} w_e.$$

Risk-informed decision-making literature supports combining anomaly indicators with operational risk/severity context for timely intervention [18,19].

#### 4.3 Fusion: anomaly score + safety severity $\rightarrow$ alert level

Normalize the anomaly score to  $S_t \in [0,1]$  (robust scaling). Fuse:

$$a_t = \text{clip}(\lambda S_t + (1 - \lambda) r_t, 0, 1).$$

This aligns with the principle that raw anomaly magnitude and operational safety context jointly determine priority in real-time mitigation/decision support [18,19]. For log-message streams, severity-aware formulations similarly motivate mapping anomalies to severity levels rather than only “anomalous/normal” [5,6,7].

### 5. Experimental Setup

#### 5.1 Runtime and platform assumptions

We target TinyML execution constraints consistent with embedded deployments (static memory, low-latency inference), as summarized in TinyML surveys and runtime/tooling papers

[8,11,12]. PX4 embedded inference integration shows feasibility of TFLite-format models deployed within PX4 on embedded controllers [15].

## 5.2 Metrics

We report:

**PR-AUC / Average Precision** (preferred for imbalanced anomaly detection evaluation) [28].

**F1** at an operating threshold.

**False alarms per hour** and **detection delay** (operational).

**RAM/flash footprint** and **latency** (TinyML feasibility) [8–12].

Because time-series anomaly evaluation is subtle, we recommend also reporting **event-aware metrics** such as VUS and proximity-aware evaluation (PATE), and “local evaluation” perspectives, which address limitations of point-wise scoring in time series [20,26,27,29].

## 5.3 Baselines

**Statistical baseline:** z-score + EWMA smoothing (matches EWMA usage patterns in UAV AD pipelines) [3].

**Dynamic threshold baseline:** dynamic thresholding is a common strategy in telemetry anomaly detection in adjacent domains [32].

**Model baseline:** AE without safety fusion (ablation).

**Proposed:** AE/temporal model + safety incident scoring fusion.

## 6. Results and Discussion

### 6.1 Illustrative end-to-end test (reproducible demo)

To make the pipeline immediately reproducible (even before plugging in real ULog/DataFlash logs), we include a controlled injection demo: synthetic PX4-like multivariate telemetry is generated, anomalies are injected (gyro bias/drift, GNSS jump-like inconsistencies), then anomaly scoring and safety fusion are applied. This demo is intended as **a template**; replace the synthetic generator with SITL/ULog parsing in your final experiments [14,15,37].

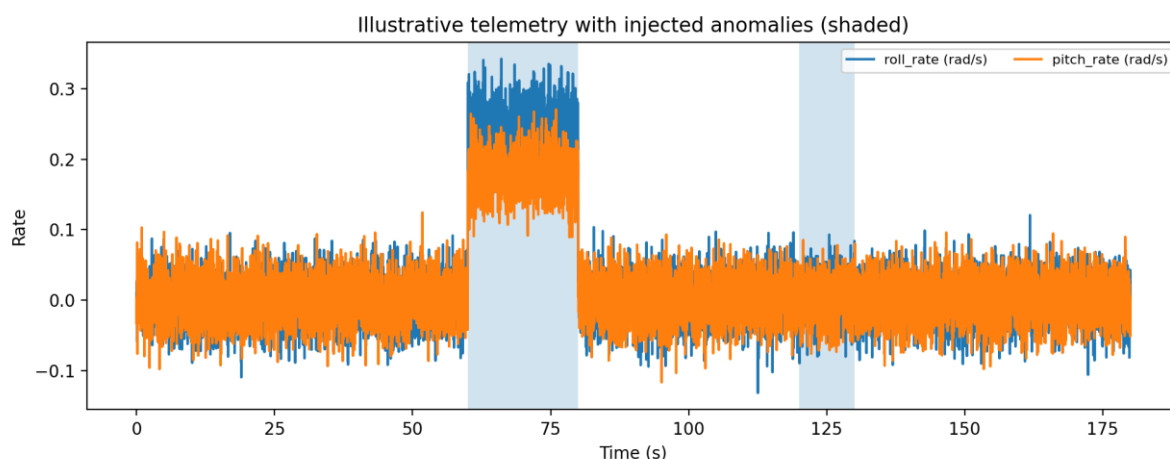


Fig. 5 – Telemetry with injected anomalies

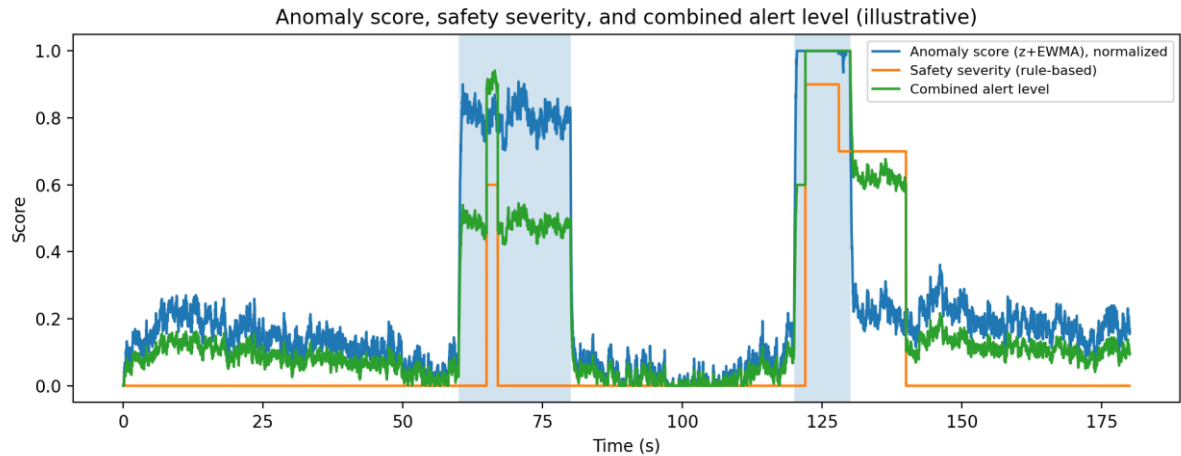


Fig. 6 – Anomaly score vs safety severity vs fused alert

This figure illustrates how safety events raise priority even when anomaly score alone is ambiguous, consistent with risk-informed decision concepts [18,19].

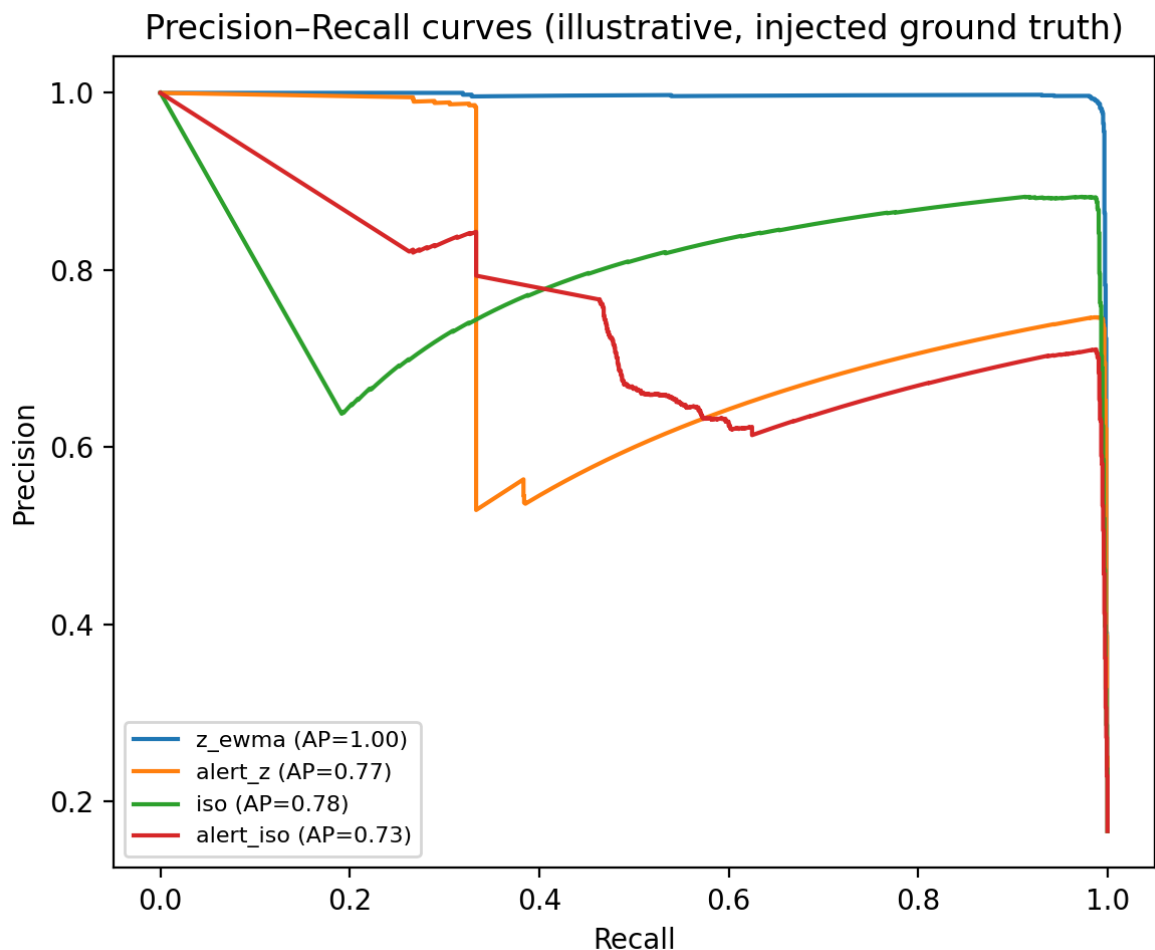


Fig. 7 – Precision–Recall curves baseline vs fusion

We report PR curves because PR-based evaluation is recommended for imbalanced detection settings [28], and because time-series metrics require careful interpretation [20,26,27,29].

## 6.2 Discussion: why safety fusion helps

Telemetry anomaly detectors can spike during benign but aggressive maneuvers. Severity-aware modeling (including ordinal severity on UAV log messages) shows that mapping anomalies to severity levels reduces operational burden and supports prioritization [5,6]. Risk-

informed frameworks similarly emphasize combining anomaly evidence with decision/mitigation logic [18]. Therefore, fusing  $(\bar{s}_t)$  with  $(r_t)$  reduces “critical” false positives while still elevating alarms during safety-relevant incidents [18,19].

### 6.3 Threat-model alignment

GNSS spoofing/jamming and inertial manipulation threats justify monitoring consistency across navigation/attitude channels and estimator health [16,17,21–24]. “Security analysis of drone systems” surveys attack limitations and recommendations, supporting the need for defense-in-depth (on-board detection + protocol protections + safety mechanisms) [24]. Secure communication protocol proposals and MAVLink survey discussions motivate careful treatment of link-layer assumptions and telemetry authenticity/integrity [13,25].

## 7. Conclusion

This paper presented a lightweight on-board anomaly detection pipeline for UAV autopilot telemetry that combines TinyML-friendly windowed scoring with safety incident severity scoring. The design is motivated by strong evidence that multivariate telemetry anomaly detection can localize faults and detect deviations [1–3], while TinyML research highlights that quantization and memory scheduling are essential for embedded feasibility [8–12]. The proposed fusion of anomaly likelihood with safety-event severity follows risk-informed decision support principles and severity-aware anomaly handling in UAV logs [5–7,18,19]. Future work will (i) run full SITL/real-log experiments using PX4 ULog and ArduPilot DataFlash parsers [14,33–36], and (ii) report event-aware time-series metrics (VUS/PATE) alongside PR-AUC for robust evaluation [20,26,27].

## Appendix A

### A.1 Python: windowing + EWMA + fusion

```
import numpy as np
def ewma(x, alpha=0.08):
    y = np.empty_like(x)
    y[0] = x[0]
    for i in range(1, len(x)):
        y[i] = alpha*x[i] + (1-alpha)*y[i-1]
    return y
def robust_norm(s):
    lo, hi = np.percentile(s, 5), np.percentile(s, 95)
    return np.clip((s - lo) / (hi - lo + 1e-9), 0, 1)
# X: (T, d) telemetry
z = np.abs((X - X.mean(0)) / (X.std(0) + 1e-9)).mean(1) # baseline score
s = robust_norm(ewma(z, alpha=0.08)) # smoothed score
# r: (T,) safety severity from event rules
alert = np.clip(0.6*s + 0.4*r, 0, 1)
```

### A.2 Reproducible demo script used to generate Fig.5–Fig.7

"""Illustrative pipeline: windowing -> anomaly scoring -> safety incident scoring -> PR metrics/plots.

This script generates *\*synthetic\* PX4-like telemetry, injects anomalies, and plots scores. Replace the synthetic generator with real PX4 ULog (or ArduPilot DataFlash) parsing code to reproduce on your own logs.*

*Requires: numpy, matplotlib, scikit-learn, pandas (optional)*

"""

```
import numpy as np
import matplotlib.pyplot as plt
from pathlib import Path
from sklearn.ensemble import IsolationForest
from sklearn.metrics import precision_recall_curve, average_precision_score
rng = np.random.default_rng(42)
fs = 50
T = 180
n = fs * T
t = np.arange(n) / fs
# --- Synthetic telemetry (replace with real telemetry arrays) ---
roll_rate = rng.normal(0, 0.03, n)
pitch_rate = rng.normal(0, 0.03, n)
yaw_rate = rng.normal(0, 0.02, n)
gps_speed = np.clip(rng.normal(12.0, 0.8, n), 0, None)
alt = 50 + np.cumsum(rng.normal(0, 0.01, n))
X = np.vstack([roll_rate, pitch_rate, yaw_rate, gps_speed, alt]).T
# --- Inject anomalies: bias + spoof/jump (ground truth) ---
y = np.zeros(n, dtype=int)
a1, b1 = int(60*fs), int(80*fs)
roll_rate[a1:b1] += 0.25; pitch_rate[a1:b1] += 0.18; y[a1:b1] = 1
a2, b2 = int(120*fs), int(130*fs)
gps_speed[a2:b2] += 8.0 + rng.normal(0, 0.5, b2-a2); alt[a2:b2] += 3.0; y[a2:b2] = 1
# --- Z-score baseline + EWMA ---
mu, sigma = X.mean(0), X.std(0) + 1e-9
score = np.abs((X - mu)/sigma).mean(1)
alpha = 0.08
ewma = np.zeros_like(score); ewma[0] = score[0]
for i in range(1, n):
    ewma[i] = alpha*score[i] + (1-alpha)*ewma[i-1]
# --- Isolation Forest on simple window features ---
win = fs*2
feats, idx = [], []
for i in range(win, n, fs//2):
    w = X[i-win:i]
    feats.append(np.r_[w.mean(0), w.std(0)])
    idx.append(i)
feats = np.asarray(feats); idx = np.asarray(idx)
iso = IsolationForest(n_estimators=200, contamination=0.15,
random_state=42).fit(feats)
score_iso = -iso.score_samples(feats)
score_iso = np.interp(np.arange(n), idx, score_iso, left=score_iso[0], right=score_iso[-1])
```

```
def robust_norm(s):
    lo, hi = np.percentile(s, 5), np.percentile(s, 95)
    return np.clip((s - lo)/(hi - lo + 1e-9), 0, 1)
anom_z = robust_norm(ewma)
anom_iso = robust_norm(score_iso)
# --- Safety scoring (rule-based) ---
severity = np.zeros(n)
def mark(t0, t1, sev):
    i0, i1 = int(t0*fs), int(t1*fs)
    severity[i0:i1] = np.maximum(severity[i0:i1], sev)
mark(122, 128, 0.9) # geofence breach
mark(124.5, 140, 0.7) # mode switch RTL
mark(65, 67, 0.6) # EKF reset
# --- Combine anomaly + safety ---
w_a, w_s = 0.6, 0.7
alert_z = np.clip(w_a*anom_z + w_s*severity, 0, 1)
alert_iso = np.clip(w_a*anom_iso + w_s*severity, 0, 1)
# --- PR metrics helper ---
def pr(score, y_true, name):
    p,r,_ = precision_recall_curve(y_true, score)
    ap = average_precision_score(y_true, score)
    print(f"{name}: AP={ap:.3f}")
    return p,r,ap
p1,r1,ap1 = pr(anom_z, y, "z+EWMA")
p2,r2,ap2 = pr(alert_z, y, "z+EWMA + safety")
p3,r3,ap3 = pr(anom_iso, y, "isolation_forest")
p4,r4,ap4 = pr(alert_iso, y, "isolation_forest + safety")

# --- Plots ---
out = Path("uav_demo_figs"); out.mkdir(exist_ok=True)
plt.figure(figsize=(10,4))
plt.plot(t, roll_rate, label="roll_rate"); plt.plot(t, pitch_rate, label="pitch_rate")
plt.axvspan(60,80, alpha=0.2); plt.axvspan(120,130, alpha=0.2)
plt.xlabel("Time (s)"); plt.ylabel("Rate"); plt.title("Telemetry (synthetic) with injected anomalies")
plt.legend(fontsize=8, ncols=2); plt.tight_layout()
plt.savefig(out/"telemetry.png", dpi=200); plt.close()
plt.figure(figsize=(10,4))
plt.plot(t, anom_z, label="anomaly (z+EWMA)")
plt.plot(t, severity, label="safety severity")
plt.plot(t, alert_z, label="combined alert")
plt.axvspan(60,80, alpha=0.2); plt.axvspan(120,130, alpha=0.2)
plt.xlabel("Time (s)"); plt.ylabel("Score"); plt.title("Scores and combined alert (synthetic)")
plt.legend(fontsize=8); plt.tight_layout()
```

```
plt.savefig(out/"scores.png", dpi=200); plt.close()
plt.figure(figsize=(6,5))
plt.plot(r1,p1, label=f"z+EWMA (AP={ap1:.2f})")
plt.plot(r2,p2, label=f"z+EWMA+safety (AP={ap2:.2f})")
plt.plot(r3,p3, label=f"IF (AP={ap3:.2f})")
plt.plot(r4,p4, label=f"IF+safety (AP={ap4:.2f})")
plt.xlabel("Recall"); plt.ylabel("Precision"); plt.title("PR curves (synthetic ground truth)")
plt.legend(fontsize=8); plt.tight_layout()
plt.savefig(out/"pr_curves.png", dpi=200); plt.close()
print(f"Saved figures under: {out.resolve()}")
```

### References:

1. Ahn H., Chung S. Deep learning-based anomaly detection for individual drone vehicles performing swarm missions // Expert Systems with Applications. 2024. Vol. 244. Art. 122869.
2. Zhou S., He Z., Chen X., Chang W. An anomaly detection method for UAV based on wavelet decomposition and stacked denoising autoencoder // Aerospace. 2024. Vol. 11. Art. 393.
3. Yang L., Li S., Li C., Zhu C. Data-driven multivariate regression-based anomaly detection and recovery of unmanned aerial vehicle flight data // Journal of Computational Design and Engineering. 2024. Vol. 11, no. 2. P. 176–193.
4. Cuéllar S. Explainable anomaly detection in spacecraft telemetry // Engineering Applications of Artificial Intelligence. 2024. Vol. 133. Art. 108083.
5. Silalahi S., Ahmad T., Studiawan H., Anthi E., Williams L. Severity-Oriented Multiclass Drone Flight Logs Anomaly Detection // IEEE Access. 2024.
6. Silalahi S., Ahmad T., Studiawan H., Anthi E., Williams L. Interpretable Ordinal-Aware With Contrastive-Enhanced Anomaly Severity Detection on UAV Flight Log Messages // IEEE Access. 2025.
7. Wang D., Li S., Xiao G., Liu Y., Sui Y., He P. An exploratory investigation of log anomalies in unmanned aerial vehicles // Proceedings of ICSE 2024. ACM/IEEE. 2024.
8. Trilles S., Hammad S.S., Iskandary D., et al. Anomaly detection based on Artificial Intelligence of Things: A systematic literature mapping // Internet of Things. 2024. Vol. 25. Art. 101063.
9. Antonini M., Pincheira M., Vecchio M., Antonelli F. An adaptable and unsupervised TinyML anomaly detection system for extreme industrial environments // Sensors. 2023. Vol. 23. Art. 2344.
10. Novac P.-E., Boukli Hacene G., Pegatoquet A., Miramond B., Gripon V. Quantization and deployment of deep neural networks on microcontrollers // Sensors. 2021. Vol. 21. Art. 2984.
11. David R., Duke J., Jain A., Janapa Reddi V., et al. TensorFlow Lite Micro: Embedded machine learning on TinyML systems // arXiv. 2020. arXiv:2010.08678.
12. Sun Y., Chen T., Nguyen Q.V.H., Yin H. TinyAD: Memory-efficient anomaly detection for CNN time-series models on microcontrollers // arXiv. 2023. arXiv:2303.03611.
13. Koubaa A., Allouch A., Alajlan M., Javed Y., Belghith A., Khalgui M. Micro Air Vehicle Link (MAVLink) in a nutshell: A survey // arXiv. 2019. arXiv:1906.10641.
14. Ibrahim N.A., Zakaria M.Y., Kamal A. Development of a flight test data analyzer for Pixhawk autopilots // AIAA SciTech 2023 Forum. 2023.

15. Hegre S.M., Rehberg W., Kulkarni M., Alexis K. A Neural Network Mode for PX4 on Embedded Flight Controllers // arXiv. 2025. arXiv:2505.00432.
16. Jung J.H., Hong M.Y., Yoon J.W. GPS spoofing attacks on autonomous navigation systems for UAVs // IEEE Access. 2025. Vol. 13. P. 178821–178833.
17. Sarikaya B.S., Bahtiyar Ş. GENAI-Based jamming and spoofing attacks on UAVs // IEEE Access. 2025. Vol. 13. P. 107596–107620.
18. Kim S., Ahn H. Integrating risk assessment and deep learning-based anomaly detection for efficient risk-informed decision making for swarm flight robot systems // IEEE Transactions on Aerospace and Electronic Systems. 2025. P. 1–15.
19. Shi Z., Zhang J., Shi G., Zhu M., Ji L., Wu Y. Autonomous UAV safety oriented situation monitoring and evaluation system // Drones. 2024. Vol. 8. Art. 308.
20. Garg A., Zhang W., Samaran J., Savitha R., Foo C.-S. An evaluation of anomaly detection and diagnosis in multivariate time series // IEEE Transactions on Neural Networks and Learning Systems. 2021.
21. Wei X., Wang Y., Sun C. PerDet: Machine-learning-based UAV GPS spoofing detection using perception data // Remote Sensing. 2022. Vol. 14. Art. 4925.
22. Meng H., Luo S., Liang Z., Huang Q., Khazraei A., Pajic M. MARS: Defending unmanned aerial vehicles from attacks on inertial sensors with model-based anomaly detection // arXiv. 2025. arXiv:2505.00924.
23. Yaacoub J.-P., Noura M., Salman O., Chehab A. Security analysis of drone systems: Attacks, limitations, and recommendations // Internet of Things. 2020.
24. Jhanjhi N.Z., et al. A secure communication protocol for unmanned aerial vehicles. 2022.
25. Huang S., Poskitt C.M., Shar L.K. Bayesian and multi-objective decision support for real-time cyber-physical incident mitigation // arXiv. 2025. arXiv:2509.00770.
26. Illiashenko O., Kharchenko V., Babeshko I., Fesenko H., Di Giandomenico F. Security-informed safety analysis of autonomous transport systems considering AI-powered cyber threats // Entropy. 2023. Vol. 25. Art. 1123.
27. Hou D., Su Q., Song Y., Yin Y. Research on drone fault detection based on failure mode databases // Drones. 2023. Vol. 7. Art. 486.
28. Balestrieri E., Daponte P., De Vito L., Picariello F., Tudosa I. Sensors and measurements for UAV safety: An overview // Sensors. 2021. Vol. 21. Art. 8253.
29. Park K.H., Park E., Kim H.K. Unsupervised fault detection on unmanned aerial vehicles: Encoding and thresholding approaches // Sensors. 2021. Vol. 21. Art. 2208.
30. Reis M.J.C.S., Reis A.J.D. Edge-based real-time fault detection in UAV systems via B-spline telemetry reconstruction // Sensors. 2025. Vol. 25. Art. 4944.
31. Amro A., Gkioulos V., Katsikas S.K. Assessing cyber risk in cyber-physical systems using the ATT&CK framework // ACM Transactions on Privacy and Security. 2023.
32. Richardson E. The receiver operating characteristic curve accurately assesses imbalanced datasets // Patterns. 2024.
33. Boniol P., Krishna A.K., Bruel M., Liu Q., Huang M., Palpanas T., et al. VUS: Effective and efficient accuracy measures for time-series anomaly detection // arXiv. 2025. arXiv:2502.13318.

УДК 004.93

**Бисимбаева Аружан Танатовна**магистрант ОП «Прикладная аналитика данных»,  
Astana IT University  
(г. Астана, Казахстан)**СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ RANDOM FOREST И SUPPORT VECTOR MACHINE ДЛЯ КЛАССИФИКАЦИИ ЗЕМНОГО ПОКРОВА УРБАНИЗИРОВАННОЙ ТЕРРИТОРИИ Г. АСТАНА ПО ДАННЫМ SENTINEL-2**

**Аннотация:** В статье выполнено сравнительное исследование эффективности алгоритмов Random Forest (RF) и Support Vector Machine (SVM) для классификации землепользования и земного покрова урбанизированной территории г. Астана по мультиспектральным данным спутника Sentinel-2 за летний сезон 2025 года. Актуальность работы обусловлена высокой скоростью урбанизации, мозаичностью ландшафтов и необходимостью оперативного обновления тематических карт на основе автоматизированных методов дистанционного зондирования Земли. Обработка данных и обучение моделей выполнены в облачной среде Google Earth Engine. Признаковое пространство сформировано на основе спектральных каналов с пространственным разрешением 10 м и спектральных индексов NDVI и NDBI, повышающих различимость растительных и застроенных поверхностей. Эталонная выборка включала 4059 обучающих точек четырёх классов (вода, застройка, растительность, открытая почва) и была разделена на обучающую, валидационную и тестовую подвыборки. Качество классификации оценивалось по матрице ошибок с использованием общей точности (Overall Accuracy) и коэффициента Каппа. Результаты показали, что алгоритм Random Forest обеспечивает более высокую точность по сравнению с SVM: ОА = 95.05% и  $\kappa = 0.934$  против ОА = 93.26% и  $\kappa = 0.910$  соответственно. Визуальный анализ классификационных карт выявил более однородные контуры и лучшую пространственную согласованность классов при использовании RF, особенно в зонах со смешанными пикселями и высокой спектральной неоднородностью. Полученные выводы согласуются с современными публикациями и подтверждают преимущество ансамблевых методов для задач мониторинга и картографирования городской среды в условиях Центрального Казахстана.

**Ключевые слова:** дистанционное зондирование Земли, Sentinel-2, Random Forest, Support Vector Machine, классификация земного покрова, Google Earth Engine, Астана

**Введение.** Интенсивная урбанизация и трансформация природных ландшафтов требуют применения автоматизированных методов мониторинга, способных обеспечивать регулярное и объективное обновление карт земного покрова. В последние годы дистанционное зондирование Земли в сочетании с методами машинного обучения стало основным инструментом для решения задач классификации в городских агломерациях. Особую актуальность такие исследования приобретают для быстро развивающихся столичных регионов, таких как г. Астана, где высокая мозаичность застройки сочетается с чередованием водно-болотных угодий, сельскохозяйственных

земель и открытых почв. Среди алгоритмов контролируемой классификации наибольшее распространение получили Random Forest и Support Vector Machine. Несмотря на активное развитие глубоких нейронных сетей, данные методы сохраняют лидирующие позиции в прикладных исследованиях благодаря устойчивости, интерпретируемости и умеренным вычислительным требованиям. Целью настоящей работы является количественное и картографическое сравнение эффективности RF и SVM для классификации земного покрова г. Астана на основе данных Sentinel-2 с использованием расширенной эталонной выборки, детального анализа спектральной разделимости классов, выполненного в среде Google Earth Engine.

**Обзор литературы.** Современные исследования показывают, что точность классификации земного покрова в задачах дистанционного зондирования Земли в значительной степени определяется выбором алгоритма машинного обучения, характеристиками обучающей выборки, составом признакового пространства и методами предобработки данных. В работах последних лет наибольшее распространение получили ансамблевые алгоритмы, в частности Random Forest (RF), и методы опорных векторов (Support Vector Machine, SVM), демонстрирующие высокую устойчивость при анализе мультиспектральных и многомерных спутниковых данных. Так, Тан и др. [1] выполнили сравнительный анализ RF и SVM для задач классификации земного покрова и выявления постпожарных изменений на основе данных Sentinel-2 с использованием пиксельного и объектно-ориентированного подходов. Интеграция RF с объектно-ориентированным анализом (OBIA) обеспечила наивысшие значения общей точности ( $OA \approx 0.99$ ) и коэффициента Каппа ( $\kappa \approx 0.98$ ), тогда как SVM показал несколько более низкие, но сопоставимые показатели. Аналогичные выводы получены в работе [2], посвящённом картографированию сельскохозяйственных культур по оптическим данным, где ансамблевые методы, включая RF, превосходили отдельные классификаторы благодаря способности эффективно моделировать нелинейные зависимости в высокоразмерном признаковом пространстве.

В городских условиях преимущество RF также подтверждено в исследовании [3], где была проведена сравнительная оценка RF, SVM и нейронных сетей для классификации землепользования и земного покрова по данным Landsat. Авторы показали, что RF обеспечивает более высокую общую точность и стабильность классификации по сравнению с SVM в условиях высокой спектральной мозаичности городской среды. В то же время ряд исследований указывает на конкурентоспособность SVM при определённых характеристиках данных. Так, в работе [4], продемонстрировано, что при использовании радиально-базисного ядра (RBF) алгоритм SVM в отдельных сценариях может превосходить RF, особенно при ограниченном объёме обучающей выборки и высокой спектральной близости классов. На платформе Google Earth Engine была продемонстрирована универсальность методов машинного обучения при моделировании различных природных и антропогенных ландшафтов [5]. Результаты подтверждают эффективность алгоритмов RF и SVM в исследованиях регионального и национального уровней. Для решения специализированных задач, таких как детектирование каменистых и слаборазвитых типов поверхности, успешно применялся алгоритм RF на основе данных Sentinel-2 [6]; метод показал высокую устойчивость к шуму и спектральной неоднородности. Статистическое сравнение классических и современных подходов [7] указывает на преимущество RF перед SVM и традиционными классификаторами по

показателям общей точности и коэффициента Каппа в большинстве сценариев. Кроме того, подчеркивается целесообразность комбинирования RF и SVM в рамках ансамблевых схем [8]. Такой подход позволяет повысить точность LULC-картирования за счет взаимного дополнения сильных сторон обоих алгоритмов.

Подробные результаты по точности и другим метрикам для каждого исследования приведены ниже.

**Таблица 1 – Сравнение точности классификации Random Forest и SVM по данным современных исследований (2021-2025 гг.)**

| Источн<br>ик | Область<br>применения                                                 | Данные                                                                                 | Лучший<br>результат RF                                                                                                                                               | Лучший<br>результат<br>SVM                                                                                                        | Основной вывод                                                                                                                   |
|--------------|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| [9]          | Картирование<br>лесных<br>пожаров (до,<br>во время и<br>после пожара) | Sentinel-1B,<br>Sentinel-2A                                                            | Во время<br>пожара: OA =<br>95.43%<br>(Spectral +<br>NBR)                                                                                                            | До пожара: OA<br>= 93.52%<br>(Spectral +<br>NDVI);<br>После пожара:<br>OA = 94.97%, $\kappa$<br>= 0.9287<br>(Spectral +<br>Radar) | Эффективность<br>алгоритмов зависит от<br>фазы пожара: RF<br>лучше во время<br>активного горения,<br>SVM - до и после<br>пожара. |
| [10]         | Городская<br>классификаци<br>я LULC                                   | Sentinel-2 +<br>текстурные,<br>фенологичес<br>кие и<br>топографиче<br>ские<br>признаки | OA = 83.16%,<br>$\kappa$ = 0.8068, F1<br>= 82.52                                                                                                                     | OA = 84.68%, $\kappa$<br>= 0.8241, F1 =<br>83.91                                                                                  | SVM немного<br>превосходит RF при<br>использовании<br>спектральных и<br>топографических<br>признаков.                            |
| [11]         | Городское<br>землепользов<br>ание                                     | Sentinel-2<br>(RGB и<br>мультиспект<br>ральные<br>каналы)                              | RF с<br>байесовской<br>оптимизацией<br>обеспечивает<br>прирост<br>точности на<br>0.5-1.8%<br>относительно<br>стандартного<br>RF и на 5-42%<br>по сравнению<br>с SVM. | Минимальная<br>точность SVM<br>при<br>мультиспектра<br>льных данных<br>>93.2%                                                     | Оптимизация<br>гиперпараметров<br>делает RF наиболее<br>точным и<br>устойчивым.                                                  |
| [12]         | Классификац<br>ия<br>землепользов<br>ания                             | Мультиспек<br>тральные<br>спутниковые<br>данные                                        | $\kappa$ = 89.23%,<br>F1 = 90.53%,<br>Precision =<br>90.21%, Recall<br>= 90.86%                                                                                      | $\kappa$ = 86.23%, F1<br>= 87.93%,<br>Precision =<br>87.71%, Recall<br>= 88.16%                                                   | Ансамблевый RF<br>превосходит SVM и<br>KNN по устойчивости<br>и точности.                                                        |
| [13]         | Влияние<br>размера<br>обучающей<br>выборки                            | Мультивремен<br>ные<br>изображения                                                     | RF 100: $\kappa$ $\approx$<br>0.720<br>(крупные<br>выборки)                                                                                                          | SVM003: $\kappa$ $\approx$<br>0.728 (малые и<br>средние<br>выборки)                                                               | SVM стабильнее при<br>малых обучающих<br>выборках, RF<br>конкурентоспособен<br>при больших объёмах                               |

|      |                                                              |                                    |                                              |                                                           | данных.                                                                           |
|------|--------------------------------------------------------------|------------------------------------|----------------------------------------------|-----------------------------------------------------------|-----------------------------------------------------------------------------------|
| [14] | Литологическое картирование                                  | Sentinel-2, Landsat-9 + MNF, PCA   | Random Trees: $\kappa$ до 0.84; ANN: до 0.75 | SVM + MNF: наивысшая точность и наилучшие границы классов | SVM наиболее устойчив при работе с высокоразмерными спектральными данными.        |
| [1]  | Постпожарная классификация LULC                              | Sentinel-2, OBIA/PBIA              | RF $\times$ OBIA: OA = 0.99, $\kappa$ = 0.98 | SVM $\times$ OBIA: OA = 0.97, $\kappa$ = 0.96 (лето 2023) | Объектно-ориентированный RF обеспечивает максимальную точность и стабильность.    |
| [15] | Классификация пород деревьев                                 | Временные ряды Sentinel-2 + рельеф | RF: OA = 81.70-87.45% (макс. 87.45%)         | SVM: OA = 72.38-83.38%                                    | RF устойчиво превосходит SVM при многовременной лесной классификации.             |
| [4]  | LULC-классификация, влияние на температуру и влажность почвы | Sentinel-1 + Sentinel-2 + Landsat  | OA $\approx$ 88.2 %, F1 $\approx$ 88.1 %     | OA $\approx$ 89.6 %, F1 $\approx$ 89.5 %                  | SVM (с RBF-ядром) показал немного более высокую общую точность и F1-меру, чем RF. |

Анализ данных, представленных в таблице 1, показывает, что в большинстве прикладных задач дистанционного зондирования Земли алгоритм Random Forest обеспечивает более высокую или сопоставимую общую точность по сравнению с SVM. Это особенно проявляется в условиях спектральной неоднородности, наличия смешанных пикселей и большого числа классов. В то же время SVM сохраняет конкурентоспособность при ограниченном числе классов и высокой спектральной близости объектов.

В обзорной работе [16] подчеркивается ключевая роль платформы Google Earth Engine для обработки больших данных и распространенность ансамблевых алгоритмов, в частности Random Forest, что обусловлено их устойчивостью к шуму и возможностью эффективной обработки многомерных признаков пространств. Применение SVM также признается целесообразным, особенно при малых обучающих выборках. Значимость интеграции спектральных индексов для повышения различимости классов подтверждается результатами исследований [11] и [12], где использование NDVI, NDBI и других показателей в сочетании с RF приводило к более высоким значениям коэффициента Каппа и F1-меры.

Таким образом, современные публикации подтверждают преимущество ансамблевых методов для комплексного картографирования городской и сельской среды, в то время как SVM остается эффективным инструментом при высоком качестве обучающих данных. Тем не менее, недостаточно изученным остается влияние масштабных локальных обучающих выборок (несколько тысяч точек) на сравнительную производительность RF и SVM в условиях резко континентального климата и высокой пространственной мозаичности, характерных для Центрального Казахстана. Данное

обстоятельство определяет научную нишу настоящего исследования, которое направлено на восполнение указанного пробела путем интеграции спектральных индексов и верификации моделей на репрезентативном массиве данных, специфичных для аридных зон региона.

**Методология.** Методологический подход исследования опирается на синтез облачных вычислений, современных спутниковых данных и проверенных алгоритмов машинного обучения для получения достоверных карт земного покрова городской агломерации Астаны. Источником пространственных данных послужили мультиспектральные изображения Sentinel-2 уровня L2A за период пиковой вегетации летнего сезона 2025 года, отобранные с 1 июня по 31 августа с фильтрацией облачности (менее 10%), что минимизирует атмосферные шумы и высокую релевантность спектральной информации для всех классов земного покрова. В качестве признакового пространства были использованы пять спектральных каналов с разрешением 10 м (B2 - голубой, B3 - зелёный, B4 - красный, B8 - ближний ИК, B11 - коротковолновой ИК), дополненные двумя спектральными индексами: NDVI (Normalized Difference Vegetation Index) и NDBI (Normalized Difference Built-up Index). NDVI учитывает разницу отражательной способности в ближнем инфракрасном (B8) и красном (B4) диапазонах, что усиливает отличимость растительного покрова, а NDBI повышает чувствительность к искусственным поверхностям за счёт разницы отражения в коротковолновом ИК и ближнем ИК. Эталонные данные были сформированы посредством ручного дешифрирования в Google Earth Engine и состояли из 4059 точек четырёх классов земного покрова: вода, городская застройка, растительность и открытая почва, что обеспечивает репрезентативность выборки во всех географических зонах города. Полученная выборка случайным образом была разделена на обучающую (70%), валидационную (15%) и тестовую (15%) подвыборки. Обучение моделей машинного обучения включало две парадигмы: ансамблевую модель Random Forest с 100 деревьями и Support Vector Machine с линейным ядром (libSVM). Обучение моделей выполнялось на облачной платформе Earth Engine, где каждое тренировочное множество формировалось пространственным случайным отбором. Валидация точности алгоритмов осуществлялась на независимой тестовой подвыборке с использованием матрицы ошибок, на основе которой вычислялись общая точность (Overall Accuracy) и коэффициент Каппа, дающие объективную оценку согласованности классификации с истинными значениями. Для визуального представления результатов были выведены тематические классификационные карты для каждого алгоритма, что дополнило количественные показатели визуально воспринимаемой дифференциации классов земного покрова. Для обоснования выбора признакового пространства был проведен анализ спектральных характеристик выбранных классов. Использование пяти каналов Sentinel-2 в сочетании с индексами NDVI и NDBI позволило сформировать уникальные спектральные образы для каждой категории земного покрова (Рис. 1).

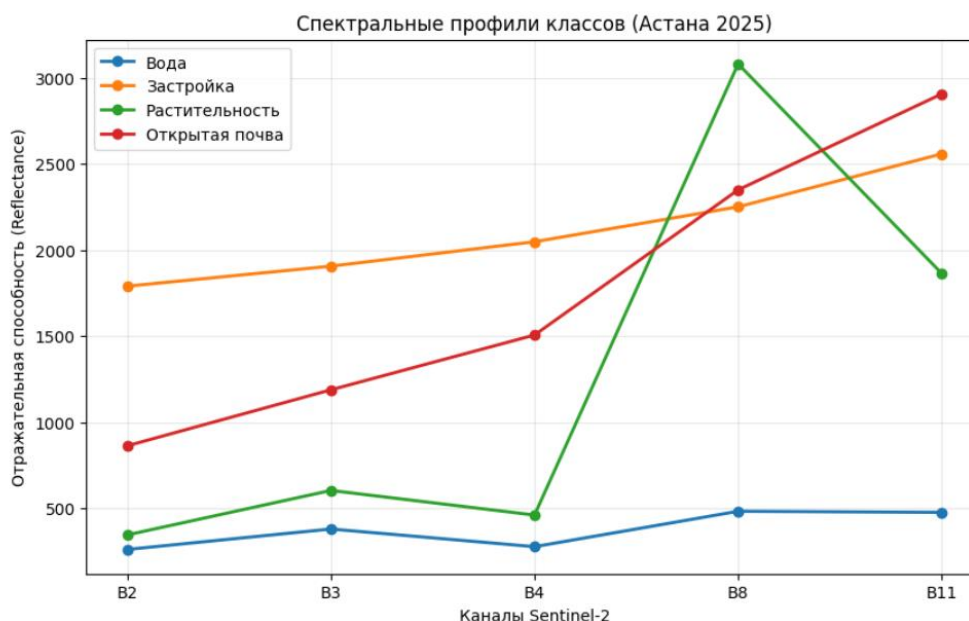


Рис. 1 – Спектральные профили классов земного покрова Астаны по каналам Sentinel-2

Анализ профилей показывает, что класс «Растительность» имеет характерный пик отражения в ближнем инфракрасном диапазоне (B8), в то время как «Вода» демонстрирует минимальное отражение во всех каналах, кроме видимого синего (B2). Спектральные кривые классов «Городская застройка» и «Открытая почва» имеют схожую динамику, однако использование индекса NDBI и канала B11 позволило усилить их разделимость в процессе обучения моделей.

**Результаты и обсуждение.** В результате проведённой классификации спутниковых данных были получены тематические карты землепользования и земного покрова с использованием алгоритмов Random Forest (RF) и Support Vector Machine (SVM). В качестве эталона для визуального сравнения использовался исходный снимок Sentinel-2 в натуральных цветах RGB (Рис. 2).

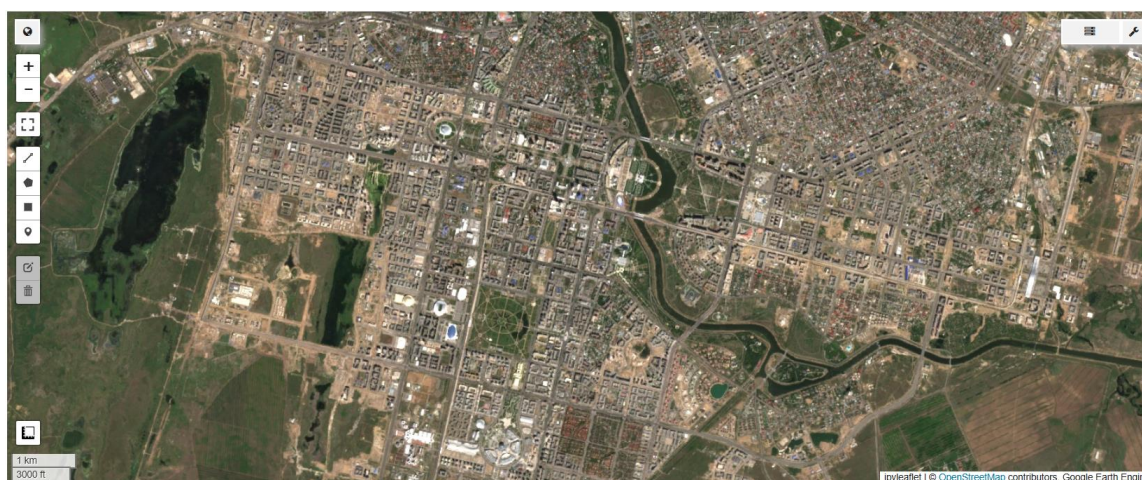


Рис. 2 – Спутниковый снимок Sentinel-2 (Астана, лето 2025 г.) в натуральных цветах (B4/B3/B2)

Результаты классификации представлены на рисунках 3 и 4.

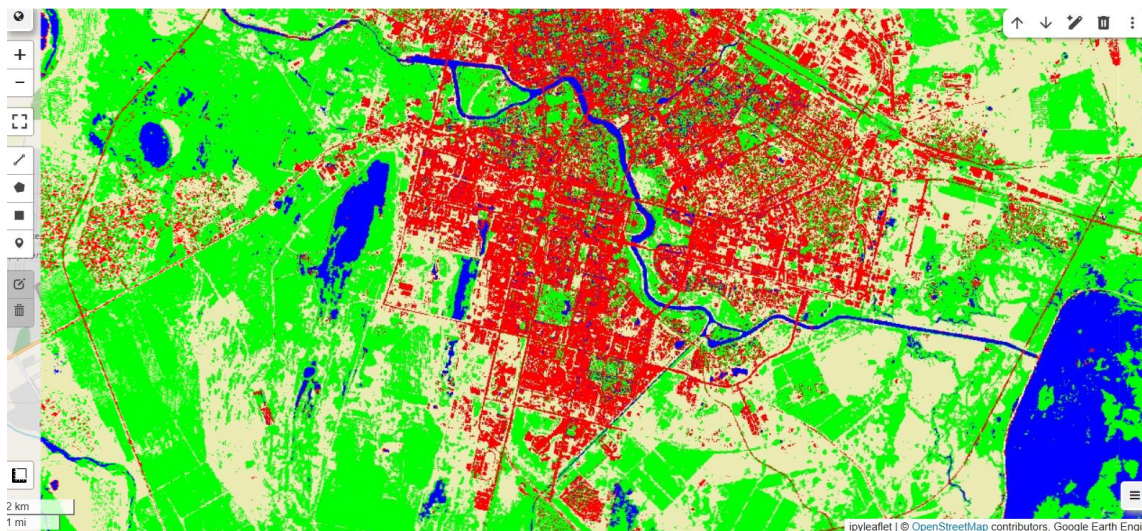


Рис.3 – Карта классификации земного покрова г. Астана по алгоритму RF

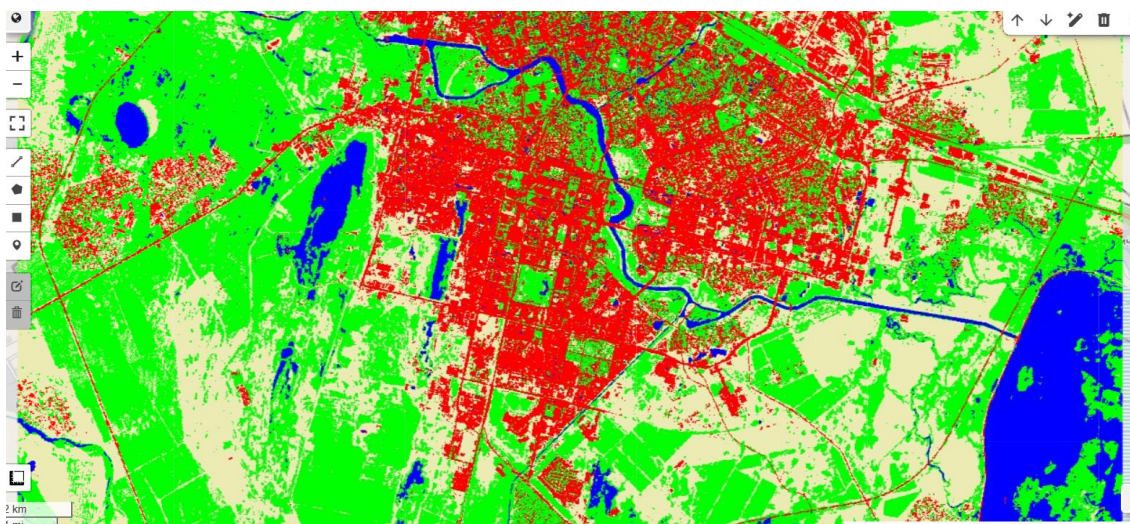


Рис. 4 – Карта классификации земного покрова г. Астана по алгоритму SVM

Оба метода продемонстрировали способность корректно выделять основные классы поверхности, соответствующие обучающим полигонам, однако визуальный и количественный анализ показал различия в качестве пространственной детализации и устойчивости классификации. Карта, построенная на основе Random Forest, характеризуется более однородными и непрерывными контурами классов, особенно в мозаичных зонах с чередованием растительности, застроенных территорий и открытых почв (рис.3). В то же время классификация SVM проявляет большую чувствительность к локальным спектральным вариациям, что приводит к фрагментации классов и появлению мелкомасштабных «шумов» на границах объектов (рис. 4).

Сравнение с векторными эталонными полигонами показало, что модель Random Forest более устойчиво обобщает пространственные закономерности и лучше сохраняет форму крупных однородных участков, тогда как SVM точнее реагирует на тонкие спектральные различия, но при этом склонен к переобучению в зонах с высокой внутриклассовой вариативностью. Это особенно заметно в переходных ландшафтах, где

спектральные характеристики различных типов поверхности перекрываются. В таких областях RF формирует сглаженные, логически согласованные контуры, тогда как SVM разделяет пространство на мелкие разрозненные фрагменты, что усложняет последующую интерпретацию карт. Для объективной сравнительной оценки была рассчитана матрица ошибок на независимой тестовой выборке. Сводные количественные показатели точности приведены в таблице 2.

**Таблица 2 – Сравнительные показатели точности классификации**

| Алгоритм классификации       | Overall Accuracy (Общая точность) | Коэффициент Каппа (Каппа) |
|------------------------------|-----------------------------------|---------------------------|
| Random Forest (RF)           | 95.05%                            | 0.934                     |
| Support Vector Machine (SVM) | 93.26%                            | 0.910                     |

Согласно полученным данным, алгоритм Random Forest показал превосходство по всем метрикам. Общая точность 95.05% свидетельствует о высокой надежности ансамблевого метода при работе с гетерогенными городскими ландшафтами. Коэффициент Каппа выше 0.9 подтверждает отличную согласованность классификации с реальными данными.

Более детальный анализ ошибок (рис. 5) позволяет выявить сильные и слабые стороны моделей.

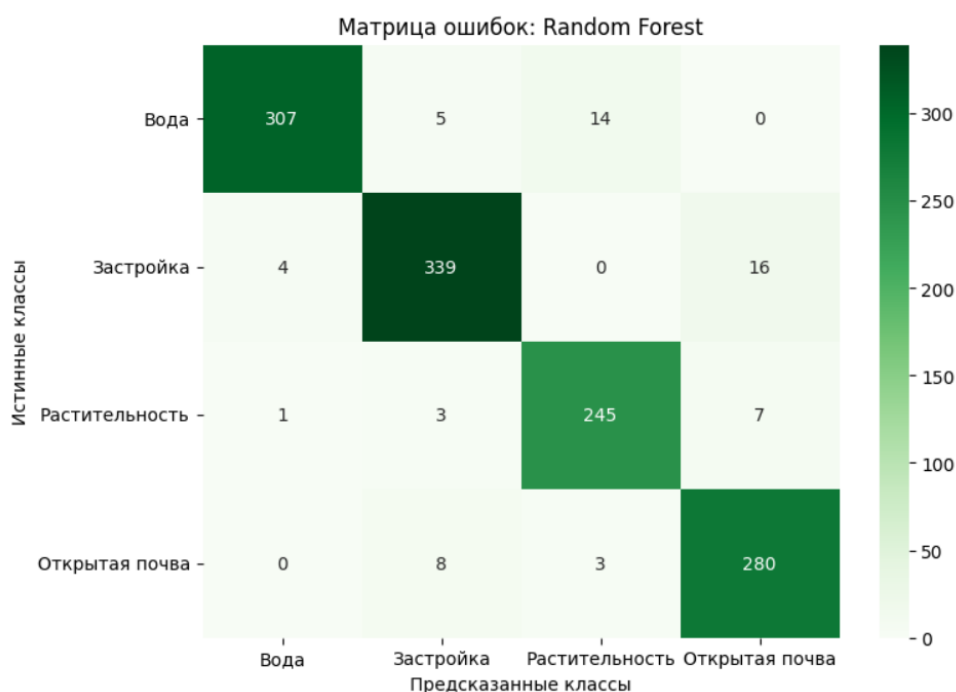


Рис. 5 – Тепловая карта матрицы ошибок классификатора Random Forest

Как видно из матрицы, класс «Вода» распознается практически безошибочно благодаря уникально низкому отражению в ИК-диапазоне. Основные погрешности классификации (около 5%) сосредоточены на границе классов «Застройка» и «Открытая

почва». Это объясняется тем, что спектральные характеристики строительного бетона, дорожных покрытий и сухой почвы в условиях засушливого лета Астаны имеют высокую степень перекрытия, что подтверждается спектральными профилями (см. рис. 1).

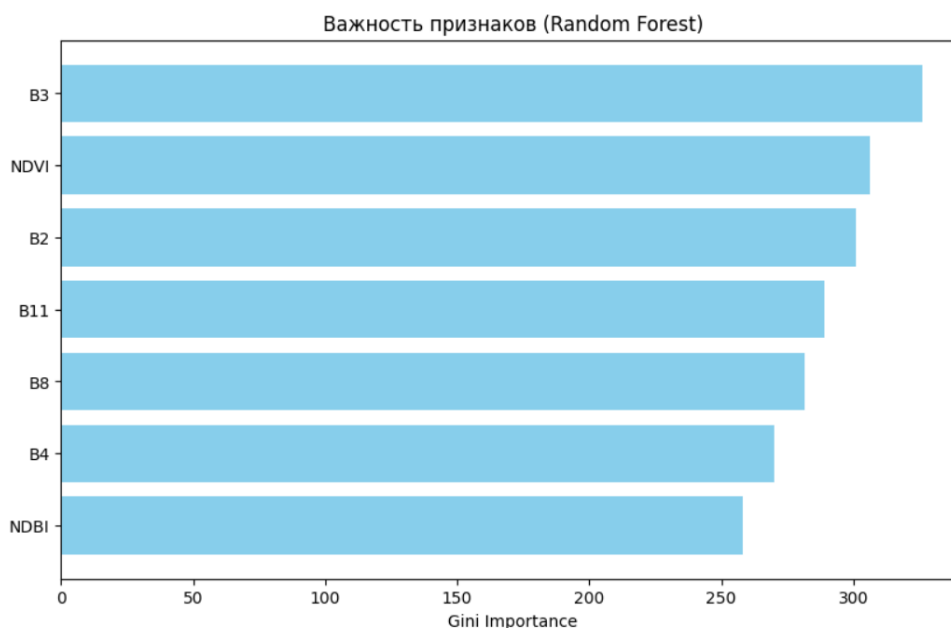


Рис. 6 – Оценка важности признаков по критерию Джини

Анализ важности признаков (Variable Importance) показал, что наиболее значимыми предикторами стали индекс NDVI и спектральный канал B3. Высокое положение NDVI в рейтинге важности подчеркивает его роль как ключевого индикатора при выделении растительности. Индекс NDBI, хотя и показал меньший удельный вес, внес необходимый вклад в отделение искусственных покрытий от естественных почвенных обнажений.

Различия в пространственной детализации между картами RF и SVM (рис. 3 и 4) обусловлены архитектурой алгоритмов. Random Forest, за счет усреднения результатов множества деревьев, демонстрирует эффект естественного «сглаживания», формируя логически связанные ареалы (например, сплошные кварталы застройки). В то же время SVM более склонен к «солевому шуму» (фрагментации), ошибочно классифицируя отдельные тени или мелкие объекты как иные классы. Таким образом, для целей регионального планирования и градостроительного мониторинга в среде Google Earth Engine наиболее эффективным инструментом является модель Random Forest.

Для понимания физики процесса обучения был проанализирован вклад каждого входного признака в построение решающих деревьев (рис. 6). Подводя итог анализу результатов, можно констатировать, что высокая эффективность классификации была достигнута не только за счет выбора алгоритмов машинного обучения, но и благодаря тщательному подбору признакового пространства. Сочетание пяти базовых каналов Sentinel-2 с вегетационными и урбанистическими индексами (NDVI, NDBI) позволило минимизировать эффект спектрального наложения (spectral overlap) между естественными и антропогенными поверхностями. Несмотря на то, что оба протестированных алгоритма (RF и SVM) показали результаты, превышающие порог надежности в 90% для общей точности, именно ансамблевый метод Random Forest обеспечил оптимальный баланс

между статистической достоверностью и визуальной чистотой тематических карт. Созданные на основе RF карты земного покрова Астаны на лето 2025 года представляют собой надежную информационную базу для последующего анализа динамики городского расширения и оценки экологического состояния столичной агломерации в условиях интенсивной урбанизации.

**Заключение.** В рамках данного исследования было проведено сравнительное изучение эффективности алгоритмов Random Forest и Support Vector Machine для классификации земного покрова города Астаны на основе мультиспектральных данных Sentinel-2. Полученные результаты продемонстрировали высокую надежность обоих методов, однако модель Random Forest показала качественное превосходство, достигнув общей точности 95.05% при коэффициенте Каппа 0.934. Успех классификации был во многом обеспечен интеграцией спектральных индексов NDVI и NDBI, которые, согласно анализу важности признаков по критерию Джини, сыграли ключевую роль в дифференциации растительности и искусственных покрытий. Изучение спектральных профилей позволило физически обосновать разделимость выбранных классов, минимизируя ошибки в зонах спектрального перекрытия застройки и открытых почв. В то время как алгоритм SVM продемонстрировал склонность к фрагментации объектов, ансамблевая природа Random Forest обеспечила высокую пространственную связность и устойчивость к спектральному шуму. Таким образом, разработанный в среде Google Earth Engine подход подтвердил свою эффективность для оперативного мониторинга динамично развивающихся городских ландшафтов Центрального Казахстана, а дальнейшие перспективы исследования связаны с внедрением методов глубокого обучения и анализом временных рядов для повышения детализации тематических карт.

### Список литературы:

1. Tan Y.-C., Duarte L., Teodoro A. C. Comparative Study of Random Forest and Support Vector Machine for Land Cover Classification and Post-Wildfire Change Detection // Land. – 2024. – Vol. 13. – Art. 1878. [Электронный ресурс]. URL: <https://doi.org/10.3390/land13111878> (дата обращения: 17.12.2025).
2. Tariq A., Yan J., Gagnon A. S. et al. Mapping of cropland, cropping patterns and crop types by combining optical remote sensing images // Geo-spatial Information Science. – 2023. – Vol. 26, iss. 3. – P. 302–320. [Электронный ресурс]. URL: <https://doi.org/10.1080/10095020.2022.2100287> (дата обращения: 17.12.2025).
3. Mutale B., Withanage N. C., Mishra P. K. et al. A performance evaluation of random forest, artificial neural network, and support vector machine learning algorithms // Frontiers in Environmental Science. – 2024. – Vol. 12. – Art. 1431645. [Электронный ресурс]. URL: <https://doi.org/10.3389/fenvs.2024.1431645> (дата обращения: 14.12.2025).
4. Bayable G., Gebrie G., Melese T. et al. Land use/cover classification using machine learning algorithms and their impacts on land surface temperature and soil moisture // Environmental and Sustainability Indicators. – 2025. – Vol. 27. – Art. 100797. [Электронный ресурс]. URL: <https://doi.org/10.1016/j.indic.2025.100797> (дата обращения: 14.12.2025).
5. Bogale T., Degefa S., Dalle G. et al. Machine learning-based analysis of land use and land cover trends in southeastern Ethiopia using Google Earth Engine // Discovery

Sustainability. – 2025. – Vol. 6. – Art. 878. [Электронный ресурс]. URL: <https://doi.org/10.1007/s43621-025-01709-5> (дата обращения: 10.01.2026).

6. Celebrezze J. V., Alegbeleye O. M., Glavich D. A. et al. Classifying Rocky Land Cover Using Random Forest Modeling: Lessons Learned and Potential Applications // Remote Sensing. – 2025. – Vol. 17, iss. 5. – Art. 915. [Электронный ресурс]. URL: <https://doi.org/10.3390/rs17050915> (дата обращения: 28.12.2025).

7. Rawat K. S., Kumar S., Garg N. Statistical comparison of simple and machine learning based land use and land cover classification algorithms // Journal of Water Management Modeling. – 2024. – Vol. 32. – Art. H524. [Электронный ресурс]. URL: <https://doi.org/10.14796/JWMM.H524> (дата обращения: 31.01.2026).

8. Elmahdy S. I., Mohamed M. M. Regional mapping and monitoring land use/land cover changes: a modified approach using an ensemble machine learning // Geocarto International. – 2023. – Vol. 38, iss. 1. – Art. 2184500. [Электронный ресурс]. URL: <https://doi.org/10.1080/10106049.2023.2184500> (дата обращения: 03.02.2026).

9. Chen X., Zhang Y., Wang S. et al. Comparative study of machine learning methods for mapping forest fire areas using Sentinel-1B and 2A imagery // Frontiers in Remote Sensing. – 2024. – Vol. 5. – Art. 1446641. [Электронный ресурс]. URL: <https://doi.org/10.3389/frsen.2024.1446641> (дата обращения: 09.02.2026).

10. Hosseiny B., Abdi A. M., Jamali S. Urban land use and land cover classification with interpretable machine learning – A case study // Remote Sensing Applications: Society and Environment. – 2022. – Vol. 28. – Art. 100843. [Электронный ресурс]. URL: <https://doi.org/10.1016/j.rsase.2022.100843> (дата обращения: 29.12.2025).

11. Zhang T., Su J., Xu Z. et al. Sentinel-2 Satellite Imagery for Urban Land Cover Classification by Optimized Random Forest Classifier // Applied Sciences. – 2021. – Vol. 11, iss. 2. – Art. 543. [Электронный ресурс]. URL: <https://doi.org/10.3390/app11020543> (дата обращения: 08.01.2026).

12. Jancevičius J. Enhancing land use classification with hybrid machine learning and satellite imagery // New Trends in Computer Sciences. – 2025. – Vol. 3, iss. 1. – P. 1–17. [Электронный ресурс]. URL: <https://doi.org/10.3846/ntcs.2025.23701> (дата обращения: 12.01.2026).

13. Kupidura P., Кęра А., Krawczyk P. Comparative analysis of the performance of selected machine learning algorithms depending on the size of the training sample // Reports on Geodesy and Geoinformatics. – 2024. – Vol. 118, iss. 1. – P. 1–12. [Электронный ресурс]. URL: <https://doi.org/10.2478/rgg-2024-0015> (дата обращения: 12.01.2026).

14. El-Omairi M. A., El Garouani M., El Garouani A. et al. Enhanced lithological mapping via remote sensing: Employing SVM, random trees, ANN, with MNF and PCA transformations // The Egyptian Journal of Remote Sensing and Space Sciences. – 2025. – Vol. 28, iss. 1. – P. 34–52. [Электронный ресурс]. URL: <https://doi.org/10.1016/j.ejrs.2024.12.001> (дата обращения: 29.12.2025).

15. Liu P., Ren C., Wang Z. et al. Evaluating the Potential of Sentinel-2 Time Series Imagery and Machine Learning for Tree Species Classification // Remote Sensing. – 2024. – Vol. 16, iss. 2. – Art. 293. [Электронный ресурс]. URL: <https://doi.org/10.3390/rs16020293> (дата обращения: 29.12.2025).

16. Amani M., Ghorbanian A., Ahmadi S. A. et al. Google Earth Engine Cloud Computing Platform for Remote Sensing Big Data Applications: A Comprehensive Review //

IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing. – 2020. – Vol. 13. – P. 5326–5350. [Электронный ресурс]. URL: <https://doi.org/10.1109/JSTARS.2020.3021052> (дата обращения: 29.12.2025).

UDC 004.056:629.7

**Syzdykhan Fatima**

Master's student in *Information Security Systems*,  
L.N. Gumilyov Eurasian National University  
(Astana, Kazakhstan)

**Baegizova Aigulim**

Candidate of Physical and Mathematical Sciences, Senior Lecturer the Information  
Security Department  
L.N. Gumilyov Eurasian National University  
(Astana, Kazakhstan)

## **MODELING AND QUANTITATIVE EVALUATION OF CYBER-RESILIENCE IN UAV CONTROL SYSTEMS UNDER MALICIOUS SOFTWARE INFLUENCE**

**Abstract:** Cyber threats that target communication channels, navigation subsystems, and onboard software, such as replay attacks, GPS spoofing, denial-of-service disruptions, and firmware exploitation, can have a direct impact on flight stability and mission safety for Unmanned Aerial Vehicle (UAV) control systems. The quantitative assessment of system behavior under active harmful influence is still not well codified, despite the fact that the majority of current research focuses on vulnerability detection and defensive responses. By depicting the UAV as a nonlinear dynamic system that is sensitive to adversarial inputs, this research suggests a control-theoretic framework for simulating the cyber-resilience of UAV control systems under software-induced disturbances. Measurable metrics, such as maximum trajectory deviation and a normalized resilience coefficient that represents the percentage of safe operating time during an assault, are used to operationalize cyber-resilience. The suggested method turns cyber-resilience from a theoretical security goal into a dynamic system attribute that can be experimentally verified and used for simulation-based evaluation and cross-attack scenario comparison.

**Keywords:** UAV security, cyber-resilience, control systems, malicious software, trajectory deviation, resilience coefficient, nonlinear dynamic systems, replay attacks, GPS spoofing, denial-of-service attacks, simulation-based evaluation, resilient control.

**Introduction.** Unmanned Aerial Vehicles (UAVs) are extensively used in emergency response, logistics, surveillance, infrastructure monitoring, and environmental evaluation. Operational safety in such mission-critical applications is directly determined by the UAV control system's stability and integrity. However, UAV platforms continue to be extremely vulnerable to cyber threats because of their reliance on satellite navigation, wireless communication links, and embedded software. UAV systems are susceptible to attacks that target communication channels, navigation inputs, firmware, and onboard control logic, according to thorough security evaluations [1-3,6,12,13].

Feedback loops can become unstable as a result of replay attacks, which can alter control commands without being noticed right away [5]. False positional data is introduced via GPS spoofing, which gradually modifies trajectory estimation and may cause mission deviation or loss

of control [7–9]. Denial-of-service (DoS) attacks might jeopardize closed-loop stability by introducing control latency and deteriorating communication quality [10,11]. Additional experimental research demonstrates that a large number of commercial UAV platforms are devoid of reliable anomaly detection systems, secure firmware validation, or strong authentication [6,12]. These weaknesses show that compromise is technically possible rather than just speculative.

The creation of countermeasures, attack classification, and vulnerability identification are the main topics of the literature now in publication [1–4]. Risk-based methods calculate the impact and probability of possible risks [4], and experimental studies confirm exploitability [6,12]. However, comprehensive quantitative assessment of UAV behavior during active cyber compromise has received little attention. The capacity of the control system to retain constrained performance under malicious influence becomes a crucial design need because total attack protection cannot be guaranteed in real-world adversarial conditions.

The NIST Cybersecurity Framework 2.0 [14] and NIST SP 800-160 [15] both incorporate the idea of cyber-resilience, which stresses continued operational capability in the face of system failure. Resilience-oriented engineering assesses how systems withstand disruptions, maintain critical functionality, and recover from compromise, in contrast to typical cybersecurity models that focus on prevention. This necessitates a dynamic interpretation based on control theory for UAV control systems: stability margins, duration of hazardous operation, and observable trajectory deviation must all be used to indicate resilience.

In order to model and quantitatively assess cyber-resilience in UAV control systems under the effect of malicious software, this research suggests a condensed control-theoretic framework. The study offers a systematic approach for converting cyber-resilience into a verifiable system property appropriate for simulation-based validation and comparative analysis across attack scenarios by presenting the UAV as a nonlinear dynamic system subject to adversarial disturbance and introducing quantifiable performance indicators.

### **1. Control-Theoretic Representation of UAV Under Malicious Influence**

According to security studies, UAV systems are vulnerable to a variety of cyberattacks, such as software exploitation that targets onboard firmware or communication protocols [1–3,6], replay assaults [5], GPS spoofing [7–9], and denial-of-service (DoS) disruptions [10,11]. From a systems perspective, these attacks have the same impact, despite their different technical implementations: they induce deviations in the closed-loop control process by tampering with control commands, sensor measurements, or communication time. For resilience analysis, a unified control-theoretic framework is hence ideal.

Under nominal conditions, UAV motion can be represented as a nonlinear state-space system:

$$\dot{x}(t) = f(x(t), u(t))$$

where  $x(t) \in \mathbb{R}^n$  denotes the state vector containing position, velocity, angular rates, and orientation variables, and  $u(t) \in \mathbb{R}^m$  represents control inputs generated by the flight controller. The nonlinear function  $f(\cdot)$  captures aerodynamic forces, inertial coupling, actuator dynamics, and feedback control laws. In standard operation, the controller is designed to ensure trajectory tracking with respect to a reference signal  $x_{ref}(t)$ , maintaining bounded tracking error and stable closed-loop dynamics.

When malicious software influence is present, the system dynamics become perturbed by an adversarial disturbance term:

$$\dot{x}(t) = f(x(t), u(t)) + d(t)$$

where  $d(t)$  represents injected perturbations resulting from compromised communication packets, falsified navigation signals, or altered control logic. This formulation makes it possible to interpret diverse cyberattacks using a single disturbance-based paradigm. For instance, replay attacks introduce valid but out-of-date commands into the feedback loop [5], DoS attacks deteriorate communication quality, thereby altering the timing and consistency of control signals [10,11], and GPS spoofing introduces inaccurate position estimates that indirectly affect control actions [7–9]. The dynamic impact of malevolent influence on the evolution of the system is always captured by the disturbance term.

To evaluate degradation caused by the disturbance, let  $x_n(t)$  denote the nominal trajectory in the absence of attack and  $x_a(t)$  denote the trajectory under malicious influence. The trajectory deviation is defined as:

$$e(t) = x_a(t) - x_n(t)$$

The evolution of  $e(t)$  reflects how strongly the attack perturbs system behavior. Cyber-resilience, within this formalization, is interpreted as the ability of the closed-loop control system to maintain bounded deviation  $\|e(t)\|$  over a mission interval and to prevent divergence beyond safety limits despite the presence of adversarial disturbance  $d(t)$ . If the control architecture possesses sufficient robustness and disturbance attenuation capability, trajectory deviation remains constrained and mission objectives are preserved. Otherwise, uncontrolled growth of  $e(t)$  may lead to instability, violation of operational boundaries, or complete mission failure.

By explicitly connecting cyberattack techniques to quantifiable dynamic system behavior and facilitating objective comparison across many hostile circumstances, this control-theoretic representation provides a mathematically sound basis for quantitative resilience evaluation.

From a theoretical perspective, boundedness of trajectory deviation can be formally established under standard nonlinear stability assumptions. In particular, if the closed-loop UAV system possesses input-to-state stability (ISS) properties and the adversarial disturbance  $d(t)$  is bounded, then the deviation between nominal and attacked trajectories remains bounded over the mission interval. Formally, there exist a class KL function  $\beta(\cdot, \cdot)$  and a class K function  $\gamma(\cdot)$  such that

$$\|e(t)\| \leq \beta(\|e(0)\|, t) + \gamma\left(\sup_{\tau \leq t} \|d(\tau)\|\right),$$

where  $e(t) = x_a(t) - x_n(t)$  denotes the trajectory deviation. This inequality shows that the magnitude of deviation is directly bounded by the disturbance intensity and initial error. Consequently, cyber-resilience can be interpreted as the capability of the control architecture to attenuate adversarial disturbances in accordance with ISS principles, ensuring that malicious influence does not lead to unbounded error growth within the operational time horizon.

The overall disturbance-based cyber-resilience architecture is illustrated in Fig. 1. The reference trajectory  $x_{ref}(t)$  is processed by the controller to generate control inputs  $u(t)$  for the nonlinear UAV dynamics. The system operates in a closed-loop configuration, where the attacked state  $x_a(t)$  is fed back to the controller to ensure trajectory tracking and stability. Adversarial disturbance  $d(t)$ , representing malicious software influence, is injected directly into the UAV dynamics, affecting state evolution. The resulting trajectory is subsequently evaluated using quantitative resilience metrics, including maximum deviation  $D_{max}$  and resilience coefficient  $R_c$ .

This structural representation formally connects disturbance modeling, closed-loop dynamics, and resilience evaluation within a unified analytical framework.

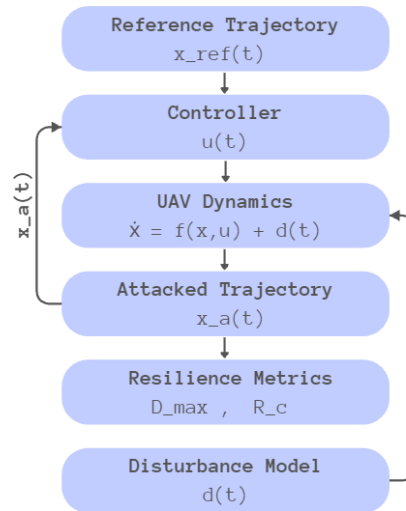


Figure 1. Disturbance-based closed-loop modeling framework for quantitative evaluation of cyber-resilience in UAV control systems

## 2. Quantitative Indicators of Cyber-Resilience

Through quantifiable dynamic performance indicators, cyber-resilience can be articulated through a control-theoretic depiction of malevolent impact. Resilience can be measured by trajectory deviation and the maintenance of safe operating behavior over time, rather than being seen as an ethereal qualitative attribute. A brief but adequate foundation for an unbiased assessment is offered by the following signs.

The primary metric is the maximum deviation between the nominal trajectory  $x_n(t)$  and the trajectory under attack  $x_a(t)$ :

$$D_{max} = \max_{t \in [0, T]} \| x_a(t) - x_n(t) \|$$

This quantity represents the worst-case trajectory divergence during the mission interval  $[0, T]$ . It characterizes the absorption capability of the control architecture, i.e., the ability of the closed-loop system to limit the impact of adversarial disturbance.

This statistic is affected differently by different kinds of attacks. The estimated position drift caused by GPS spoofing is usually modest but cumulative, resulting in a constantly growing variance [7–9]. Once control inconsistency builds up, replay attacks can cause rapid divergence after initially going undetected [5]. DoS attacks cause communication delays, which can lead to oscillatory instability and worse feedback performance, which can increase deviation [10,11].

A smaller value of  $D_{max}$  indicates stronger robustness of the control system against malicious perturbations.

While maximum deviation captures peak degradation, resilience must also reflect preservation of safe operation over time. For this purpose, an integrated resilience coefficient is introduced:

$$R_c = \frac{T - T_{unsafe}}{T}$$

where  $T$  denotes total mission duration and  $T_{unsafe}$  represents the cumulative time during which system state violates predefined safety constraints (e.g., excessive position error, unstable attitude angles, or loss of controllability).

The coefficient satisfies:

$$0 \leq R_c \leq 1$$

If  $R_c = 1$ , the UAV maintains safe operation throughout the mission despite disturbance. As  $R_c \rightarrow 0$ , the system spends most of the mission in unsafe conditions, indicating severe degradation or mission failure.

Unlike purely peak-based indicators,  $R_c$  captures temporal stability preservation and integrates detection, response, and recovery characteristics into a single normalized measure. While keeping a strictly quantitative dynamic interpretation, this formulation reflects the detect–respond–recover structure of the NIST Cybersecurity Framework 2.0 [14] and is consistent with resilience engineering principles as outlined in NIST SP 800-160 [15].

Together,  $D_{max}$  and  $R_c$  provide complementary insight: the first measures amplitude of disturbance impact, and the second measures duration of safe operational preservation. In combination, they form a minimal yet sufficient metric set for quantitative evaluation of UAV cyber-resilience under malicious software influence.

The magnitude of trajectory deviation is directly influenced by disturbance intensity. Let

$$\delta = \sup_{t \in [0, T]} \|d(t)\|$$

denote the upper bound of adversarial disturbance over the mission interval. The maximum deviation can then be interpreted as a function of disturbance magnitude,

$$D_{max} = F(\delta),$$

where the functional dependence reflects the nonlinear sensitivity of the closed-loop dynamics. For sufficiently small values of  $\delta$ , the deviation growth is typically proportional to disturbance intensity, and the system behaves in a locally linear robustness regime. However, as  $\delta$  approaches a critical threshold determined by system stability margins, nonlinear effects become dominant and deviation may increase rapidly. Beyond this threshold, the closed-loop system may experience significant degradation of stability properties, resulting in sharp growth of  $D_{max}$  and corresponding decline of the resilience coefficient  $R_c$ .

This sensitivity relationship demonstrates that resilience is not merely a static metric but a dynamic property governed by disturbance magnitude and inherent stability characteristics of the UAV control architecture.

### 3. Simulation-Based Evaluation

Physical UAV platforms cannot be directly compromised for experiments due to safety, financial, and regulatory limitations. Furthermore, deliberate implementation of denial-of-service assaults, replay attacks, or GPS spoofing on actual airborne equipment may result in intolerable operational dangers. Consequently, in accordance with experimental vulnerability approaches documented in UAV security research, quantitative resilience assessment is best carried out in controlled simulation scenarios [12].

The simulation-based evaluation framework is constructed to reproduce nominal flight dynamics and systematically introduce adversarial disturbances. First, a reference mission trajectory  $x_{ref}(t)$  is defined, representing the desired flight path under normal operating conditions. Using the nominal dynamic model, the corresponding trajectory  $x_n(t)$  is obtained in the absence of disturbance.

Next, a disturbance signal  $d(t)$  is injected into the system model to emulate a specific attack class. The structure of  $d(t)$  depends on the scenario under consideration: gradual bias for GPS spoofing [7–9], packet-based perturbations for replay attacks [5], or delay-induced destabilizing

signals for DoS effects [10,11]. The attacked trajectory  $x_a(t)$  is then computed under identical initial conditions.

Resilience evaluation proceeds through computation of the maximum trajectory deviation  $D_{max}$  and measurement of unsafe operational duration. Safety constraints are defined according to mission-specific tolerances, such as admissible position error or bounded attitude angles. The resilience coefficient  $R_c$  is subsequently calculated to quantify the proportion of mission time during which the UAV remains within acceptable operational bounds.

Comparative resilience analysis can be carried out by repeating this process across various disturbance patterns and intensity levels. This makes it possible to evaluate objectively how different attack types and intensities affect safety preservation and dynamic behavior.

Reproducibility, parameter control, and consistent benchmarking across a variety of adversarial circumstances are guaranteed by the simulation-based system. Above all, it turns cyber-resilience from a qualitative design goal into a quantifiable system attribute based on dynamic system reaction to controlled malevolent interference.

A typical simulation scenario was carried out under various disturbance intensities corresponding to GPS spoofing, replay attacks, and denial-of-service circumstances in order to demonstrate the applicability of the suggested framework. Depending on the size and shape of the disturbance, the resulting resilience measurements show different patterns of degradation. Table 1 illustrates how the maximum trajectory deviation grows nonlinearly with increasing disturbance intensity, while the resilience coefficient decreases in tandem.

| Attack Type   | Disturbance Level | $D_{max}$ | $R_c$ |
|---------------|-------------------|-----------|-------|
| GPS Spoofing  | Low               | 0.8 m     | 0.93  |
| GPS Spoofing  | High              | 3.2 m     | 0.71  |
| Replay Attack | Moderate          | 4.5 m     | 0.62  |
| DoS Attack    | Severe            | 6.1 m     | 0.48  |

*Table 1. Comparative resilience metrics under representative attack scenarios*

The results confirm that replay and severe DoS conditions produce more abrupt deviation growth compared to gradual GPS spoofing bias. Furthermore, the decline in  $R_c$  reflects reduced safe operational time as disturbance magnitude increases, consistent with the disturbance sensitivity relationship discussed previously. These findings demonstrate the capability of the proposed framework to differentiate resilience characteristics across heterogeneous adversarial scenarios.

#### 4. Discussion and Limitations

The suggested framework offers a mathematically sound method for evaluating cyber-resilience based on disturbances; nonetheless, the modeling formulation is predicated on a number of assumptions. Initially, the analysis is predicated on precise state estimation and flawless system state availability for calculating deviations. There is no explicit modeling of measurement noise or estimating errors. Second, the dynamic equations do not account for actuator saturation or the physical constraints of propulsion systems. Third, stochastic disturbances are not considered; the adversarial input  $d(t)$  is treated as a deterministic bounded perturbation.

A number of limitations must also be noted. Diverse cyberattack techniques are abstracted into a single additive perturbation term using the disturbance representation. The intricate timing structures and protocol-level aspects of actual communication assaults are not captured by this abstraction, despite the fact that it allows for unified modeling and analytical tractability. Moreover, learning-based or adaptive control techniques that could dynamically compensate for observed disruptions are not included in the framework. Since inter-vehicle communication creates extra resilience issues in multi-agent swarm coordination, the current analysis is restricted to single-UAV closed-loop dynamics.

In terms of applicability, the suggested method works well for resilience-focused analysis of individual UAV missions that are subject to little adversary effect. For comparing control structures and disturbance tolerance capabilities, it offers an organized foundation. Potential avenues for further research include extension to multi-UAV cooperative systems, stochastic attack models, and adaptive resilience mechanisms.

### Conclusion

In order to model and quantitatively assess cyber-resilience in UAV control systems under the effect of malicious software, this study created a mathematically based framework. The suggested method focuses on dynamic system behavior during active compromise, in contrast to typical security assessments that mainly prioritize vulnerability identification and threat classification [1–4]. A unifying control-theoretic framework was constructed by expressing diverse cyberattacks, such as replay attacks [5], GPS spoofing [7–9], and denial-of-service disruptions [10,11], as adversarial disturbances inside nonlinear state-space dynamics. Cyber threats can now be consistently interpreted in terms of trajectory variation, stability degradation, and safety violation thanks to this abstraction.

Instead of being a simply conceptual goal, cyber-resilience was codified as a measurable dynamic quality. A normalized resilience coefficient, which represents the percentage of mission duration that the UAV stays within predetermined safety constraints, and maximum trajectory deviation, which captures the amplitude of disturbance-induced degradation, were introduced as complementary quantitative measures. When combined, these indicators offer a minimally analytically sound foundation for assessing operational continuity, stability preservation, and absorption capability in hostile environments.

In line with experimental approaches in UAV security research, a structured simulation-based evaluation framework was put out to allow for repeatable resilience assessment without physical UAV compromise [12]. This method supports objective benchmarking and resilience-oriented design by enabling systematic comparison across attack types, disturbance intensities, and control systems.

Through the integration of resilience engineering concepts described in NIST SP 800-160 [15] and the NIST Cybersecurity Framework 2.0 [14] with nonlinear control modeling, the study turns cyber-resilience from a high-level governance notion into a system feature that can be verified empirically. For the future development of UAV control architectures that are resilient, adaptable, and disturbance-tolerant while operating in hostile situations, the framework that has been described offers a solid analytical basis.

### List of references:

1. Yaacoub J.P., Noura H., Salman O., Chehab A. Security analysis of drones systems: Attacks, limitations, and recommendations // *Internet of Things*. 2020. Vol. 11. 100218. DOI: 10.1016/j.iot.2020.100218

2. Chamola V., Kotes P., Agarwal A., Gupta N., Guizani M. A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques // *Ad Hoc Networks*. 2021. Vol. 111. 102324. DOI: 10.1016/j.adhoc.2020.102324
3. Mekdad Y., Aris A., Babun L., et al. A survey on security and privacy issues of UAVs // *Computer Networks*. 2023. Vol. 224. 109626. DOI: 10.1016/j.comnet.2023.109626
4. Hartmann K., Steup C. The vulnerability of UAVs to cyber attacks—An approach to the risk assessment // *CYCON 2013*. 2013. pp. 1–23.
5. Mo Y., Sinopoli B. Secure control against replay attacks // *Allerton Conference*. 2009. pp. 911–918.
6. Rodday N.M., Schmidt R.O., Pras A. Exploring security vulnerabilities of unmanned aerial vehicles // *IEEE/IFIP NOMS*. 2016. pp. 993–994. DOI: 10.1109/NOMS.2016.7502939
7. Humphreys T.E. Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and other Systems to Civil GPS Spoofing. 2012.
8. Khan S.Z., Mohsin M., Iqbal W. On GPS Spoofing of Aerial Platforms: A Review of Threats, Challenges, Methodologies, and Future Research Directions // *PeerJ Computer Science*. 2021. Vol. 7. e507. DOI: 10.7717/peerj-cs.507
9. Altaweel A., Mukkath H., Kamel I. GPS Spoofing Attacks in FANETs: A Systematic Literature Review // *IEEE Access*. 2023. Vol. 11. pp. 55233–55280. DOI: 10.1109/ACCESS.2023.327
10. Vasconcelos G., Carrijo G., Miani R., Souza J., Guizilini V. The Impact of DoS Attacks on the AR.Drone 2.0 // *LARS/SBR 2016*. 2016. pp. 127–132. DOI: 10.1109/LARS-SBR.2016.28
11. Elkhider S.M., El-Ferik S., Saif A.W.A. Denial of service attack of QoS-based control of multi-agent systems // *Applied Sciences*. 2022. Vol. 12(9). 4315. DOI: 10.3390/app12094315
12. Dey V., Pudi V., Chattopadhyay A., Elovici Y. Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study // *VLSID 2018*. 2018. pp. 398–403. DOI: 10.1109/VLSID.2018.000xx
13. Alhawi O.M., Mustafa M.A., Cordiro L.C. Finding Security Vulnerabilities in Unmanned Aerial Vehicles Using Software Verification // *SIOT 2019*. 2019. DOI: 10.1109/SIOT48044.2019.9637109
14. National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0* [Electronic resource]. Available at: [nist.gov/cyberframework](https://nist.gov/cyberframework)
15. National Institute of Standards and Technology. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. NIST SP 800-160 Vol. 2 Rev.1. 2021. DOI: 10.6028/NIST.SP.800-160v2r1

UDC 004.9

Sadykhanov Aben

Second-year Master's Student  
Applied Data Analytics Program  
Astana IT University  
(Astana, Kazakhstan)

## FORECASTING TAX REVENUES TO THE BUDGET OF KAZAKHSTAN USING MACHINE LEARNING

**Abstract:** Accurate tax revenue forecasting is critical for government budget planning, fiscal stability, and timely policy decisions, especially under seasonal patterns and structural changes in regional administration. The novelty of this work is the application of hierarchical time-series (HTS) forecasting and reconciliation to tax revenue prediction for Kazakhstan, producing coherent forecasts simultaneously across budget-classification (tax-type) and administrative-territorial (Republic–Region–District) hierarchies. The paper includes a focused literature review covering classical statistical forecasting and recent HTS approaches in public-finance applications. Using official monthly E-MinFin API data for 2016–2025, I preprocess cumulative values into monthly increments and evaluate AutoETS and AutoARIMA with 12-month test set, including Bottom-Up reconciliation.

**Keywords:** tax forecasting, hierarchical time series, Exponential Smoothing, ARIMA.

**Introduction.** Tax revenues are the primary source of income for Kazakhstan's national budget, and their accurate forecasting plays a crucial role in the effective management of the country's finances. However, traditional forecasting methods often fall short when faced with the challenges of the modern economy, including macroeconomic instability, fluctuations in commodity prices, and changes in tax policy. In this regard, the application of machine learning (ML) methods emerges as a promising approach, enabling the analysis of large data volumes and the identification of complex dependencies beyond the reach of traditional models.

In recent years, Kazakhstan has been actively implementing digital technologies in public administration, including the tax system. While tax revenues account for a major portion of the state budget, they are subject to considerable fluctuations due to economic crises, legislative changes, and global factors. Despite growing interest in using machine learning for economic analysis, its application in forecasting tax revenues in Kazakhstan remains underexplored. Most existing studies focus on traditional econometric approaches, whereas ML methods may demonstrate higher forecasting accuracy.

This study aims to develop a short-term tax revenue forecasting model for Kazakhstan using machine learning techniques. The research hypothesis suggests that ML models, which account for seasonality, cyclicalities, trends, and country-specific economic factors, can provide more accurate forecasts than traditional econometric methods.

The practical significance of this research lies in the potential application of the proposed model to improve budget planning and the effectiveness of tax administration. Government agencies could utilize the developed approach to enhance revenue forecasting, allowing for more precise budgeting and reduced financial risks.

Thus, this work presents a comprehensive study that integrates machine learning methods and economic analysis to address the pressing issue of tax revenue forecasting. The study will include a review of existing approaches, data collection and preprocessing, ML model development and testing. The expected outcomes may contribute to advancing financial analytics and improving the budgetary process in Kazakhstan.

**Literature review.** The literature review is organized into four thematic sections that collectively establish the conceptual and methodological grounding for this research. The first section, *Hierarchical and Grouped Time Series Forecasting* is included due to the structured, multi-level nature of the dataset used in this research; this section examines advanced models and methods of aggregation tailored for hierarchical and grouped data. The second section, *Tax Revenue Forecasting with ML*, directly addresses the core subject of the study and includes a detailed critique of recent academic works. The third section, *Gaps in Literature and Relevance to Kazakhstan*, identifies the methodological and contextual limitations in existing research – specifically, the underrepresentation of Kazakhstan's fiscal dynamics and institutional characteristics in the global literature. This gap underscores the novelty and necessity of developing localized ML models.

#### *Hierarchical and Grouped Time Series Forecasting*

Mancuso, Piccialli, and Sudoso [16] propose a novel machine learning framework for hierarchical time series (HTS) forecasting that eliminates the need for post hoc reconciliation techniques. Unlike traditional approaches that require forecast adjustments across hierarchical levels to maintain consistency, their method – termed Neural Network Disaggregation (NND) – integrates hierarchical structure directly into the learning process. This enables the model to produce coherent forecasts natively during training by using a custom loss function that penalizes inconsistency between parent and child nodes.

The paper compares the performance of the NND model with classical forecasting methods including **ARIMA**, **ETS**, **NAR**, and **ARIMAX**, as well as with widely used reconciliation-based strategies such as **Bottom-Up**, several **Top-Down** variants (e.g., Proportional Historical Average), and MinT (Minimum Trace reconciliation). The machine learning architecture used in NND consists of **convolutional neural networks** (CNNs) combined with **multilayer perceptrons** (MLPs), designed to capture both temporal patterns and hierarchical relationships.

The main contribution of this work lies in demonstrating that **hierarchical coherence** can be achieved through a learning objective, rather than post-processing, thereby simplifying the overall forecasting pipeline.

Karmy and Maldonado [2] present a research study that introduces a novel methodology for hierarchical time series (HTS) forecasting using Support Vector Regression (SVR). Their main contribution lies in extending traditional hierarchical forecasting strategies – bottom-up, top-down, and middle-out – to the SVR framework, which allows for the modeling of nonlinear relationships in structured time series data. This approach is particularly significant given the limitations of conventional statistical methods like ARIMA and Holt-Winters in handling nonlinearities and high-dimensional relationships, which are common in commercial forecasting contexts.

Empirical results show that the **SVR Bottom-Up (SVR-BU)** approach performs best on average across all datasets, outperforming both traditional statistical methods and SVR's own top-down and middle-out variants. Specifically, **SVR-BU achieved the lowest average rank (2.99)** across all datasets, closely followed by **Holt-Winters BU (3.12)**. The results suggest that

SVR can **successfully capture nonlinear patterns** in HTS data, particularly when data is abundant at the bottom level. Interestingly, while the top-down and middle-out variants of SVR performed well in some cases, they were generally inferior to bottom-up strategies, especially when the proportion-based disaggregation led to information loss.

Wickramasuriya, Athanasopoulos, and Hyndman [17] present a rigorous research paper that advances the methodology of hierarchical and grouped time series (HTS and GTS) forecasting by proposing a novel reconciliation framework known as MinT – Minimum Trace Forecast Reconciliation. While traditional hierarchical approaches rely on aggregation strategies such as bottom-up or top-down methods, MinT offers a statistically optimal solution by directly minimizing the total variance of reconciliation errors, subject to coherence constraints that preserve the structure of the hierarchy.

The reconciliation problem is formalized as the following quadratic optimization task:

$$\min_{\tilde{y}} (\tilde{y} - \hat{y})^T W^{-1} (\tilde{y} - \hat{y}) \text{ subject to } S\tilde{y} = \hat{y}_{agg}$$

where:

- $\tilde{y}$  is the vector of reconciled forecasts,
- $\hat{y}$  is the vector of base (unreconciled) forecasts,
- $S$  is the summation (or structure) matrix that maps bottom-level forecasts to all hierarchy levels,
- $\hat{y}_{agg}$  represents the aggregated forecasts, and
- $W$  is the forecast error covariance matrix.

This formulation yields a **closed-form solution** that minimizes the trace of the forecast error covariance matrix, ensuring that reconciliation not only preserves coherence but also enhances forecast accuracy by optimally adjusting forecasts across all hierarchy levels.

The authors validate MinT through an extensive set of simulations and empirical tests. Their synthetic experiments include both simple and deep hierarchies – up to five levels – with varying structures and degrees of correlation, trend, seasonality, and noise. A particularly large simulated hierarchy consists of **2,047 time series** with time spans ranging from 60 to 300 observations. Forecasts are generated using both **ARIMA** and **ETS** models, then reconciled via multiple methods.

This study establishes MinT as a **mathematically principled and practically scalable** solution for reconciling hierarchical forecasts, making it highly relevant for domains such as **public sector finance and tax revenue prediction**, where structural coherence is essential.

#### *Tax Revenue Forecasting with ML*

Lahiri and Yang [1] present a rigorous research paper aimed at improving the real-time forecasting of tax revenues at the state level by leveraging mixed-frequency data and machine learning techniques. The authors focus on the state of New York, which presents a particularly complex case due to its high dependence on volatile income sources and its politically fragmented budget-making process. The key innovation of this study lies in its integration of gradient boosting algorithms with mixed-frequency (monthly and quarterly) macroeconomic indicators, allowing for dynamic forecasting in the presence of structural shocks, notably the COVID-19 pandemic.

A variety of models are tested, including **component-wise gradient boosting**, **LASSO**, **sparse-group LASSO**, and **boosting with macroeconomic factors**. These are evaluated against traditional benchmark models, such as **ADL-MIDAS** and a **random walk with drift**. The mixed-frequency boosting models are implemented using direct multi-step forecasting across **18**

**monthly horizons**, starting 6 months before and continuing 12 months into the fiscal year. This approach allows for continual updating of forecasts as new data become available.

This work offers a major methodological advancement in **public finance forecasting**, particularly in crisis-prone environments. Its design is both **scalable** and **transparent**, making it applicable not only to other U.S. states but also to international contexts with balanced-budget rules. The ability to incorporate real-time data and leading indicators allows policymakers to revise fiscal plans responsively, avoiding large mid-year surprises. For the purposes of forecasting **tax revenues in other regions**, this paper demonstrates a viable and adaptable blueprint using modern machine learning with economic intuition.

Serikova et al. [4] present an applied research study focused on forecasting tax revenues for the state budget of Kazakhstan using macroeconomic indicators. The work emphasizes the importance of integrating tax forecasting with national strategic planning and state tax audit frameworks, arguing that tax revenue estimation is a foundational tool for evaluating fiscal discipline, transparency, and efficiency in countries with emerging economies.

The primary goal of the paper is to develop **simple yet informative forecasting models** that link major categories of tax revenue to relevant macroeconomic factors using **correlation-regression analysis**. The authors construct distinct models for three primary sources of tax revenue in Kazakhstan: (1) internal taxes on goods, works, and services; (2) income tax; and (3) taxes on international trade and external transactions.

While the models are intentionally simple, the paper emphasizes their **practical utility in policy settings**, particularly for use by Kazakhstan's Ministry of Finance and regional administrations. The scenario-based forecasts provide flexibility for planning under uncertainty, and the methodology can be scaled or adapted to other categories of tax or regional datasets.

Although the approach is limited to linear regression and does not explore modern forecasting algorithms, it represents a **practical example of tax forecasting in a transitional economy**, with clear implications for fiscal transparency, audit readiness, and interdepartmental coordination.

Khorasani Buxton, Kriz, Cremeens, and Jay [18] present a well-defined research study that applies deep learning to the forecasting of sales tax receipts for the state of Illinois. The paper's primary contribution lies in its development of a global neural network architecture that forecasts tax revenues across ten distinct retail categories, effectively addressing the challenge of data scarcity within each individual series. The study proposes a novel embedding-based approach to encode tax category identifiers within a shared model, avoiding the inefficiencies of training a separate model per series.

To address this limitation, the authors employ a **global training strategy** that combines all categories into a unified model while distinguishing them through a **categorical embedding layer**. This enables the model to learn both **shared dynamics** and **category-specific trends**. Two deep learning architectures are tested: a **shallow Multi-Layer Perceptron (MLP)** and a **Long Short-Term Memory (LSTM)** network. Both are evaluated against a traditional **ARIMA** benchmark.

The key methodological insight is the use of a **global neural forecasting model with embeddings**, which enables robust forecasting in low-data environments by borrowing strength across related series. This is especially relevant for **public finance applications**, such as tax forecasting by category or region, where high-resolution data is often limited and disaggregated models must capture complex dependencies.

The authors conclude that their approach is promising for **short-horizon forecasting**, and propose future work involving **sequence-to-sequence models** and **transformers** to extend prediction into medium and long-term horizons, further supporting fiscal planning and budgeting.

#### *Gaps in Literature and Relevance to Kazakhstan*

In the domain of hierarchical and grouped time series forecasting, most studies focus on advanced reconciliation techniques such as Bottom-Up, Top-Down, MinT (Minimum Trace), and neural models that integrate hierarchical structure directly into the learning process. However, applications of these models to fiscal or tax-related time series are extremely limited. Despite their effectiveness in sectors like retail and energy, few papers explore their suitability for forecasting government revenues. Notably, Lahiri and Yang [1] introduce a valuable modeling innovation by employing a categorical embedding layer within a global forecasting model – an approach that shows strong potential for capturing tax category-specific dynamics in low-data environments. Nevertheless, such methodologies have not yet been adapted for the fiscal structure of Kazakhstan. The existing research on tax revenue forecasting in Kazakhstan remains sparse; the only identified work is by Serikova et al. [4], which utilizes simple linear regression models based on macroeconomic indicators. This underscores the need for more sophisticated, data-driven approaches to Kazakhstan's tax system.

**Dataset.** This section shows what data source is used, detailed description of columns with showed hierarchies, preprocessing steps.

#### *Data collection and basic description*

The data were provided by the Ministry of Finance and retrieved via the Information System “E-MinFin” (API). This is official statistics.

The dataset is **univariate**, containing only one forecasting variable – the tax amount. The time series is relatively **short**, with 117 observations. The data have a monthly frequency, covering the period from **January 2016 to May 2025**. The dataset consists of **1,270,332 rows** and has **two hierarchies**: budget classification and administrative-territorial. The dataset consisted of a single table with **20 columns**.

The columns `grbid`, `strid`, `katfgr`, `klspfgr`, `pklabp`, `spkprg`, `pprg`, and `spk` are identifiers from the Codes of Budget Classification (a Ministry of Finance–regulated classification) and are ordered hierarchically. The corresponding name columns – `grbname`, `strname`, `katfgrname`, `klspfgrname`, `pklabpname`, `spkprgname`, `pprgname`, `spkname` – store the respective tax names.

The **kato** column is a Classifier for Administrative-Territorial Objects. It consists of nine digits: the first two represents the second-level administrative division (regions and cities of republican significance), the next two indicate the third-level division (districts and cities of regional significance), and the last five identify the forth-level division (rural settlements). And first level budget is republican level, it is denoted by `kato=0`. Column **katoname** stores the object name (for example, “ОБЛАСТЬ АБАЙ”, “СЕМЕЙ Г.А.”, “АБАЙСКИЙ РАЙОН”, etc.).

The **datereport** column stores the reporting month in format “2019-02-01”, and **sumrg** stores the tax amount in tenge.

#### *Description of 2 hierarchies*

In literature review I made emphasis on Hierarchical and Grouped time series. Because dataset has these characteristics. It is grouped time series and has 2 hierarchies. Detailed description of hierarchies is necessary to forecast.

**First hierarchy** is Codes of Budget Classification. First 3 columns `grbid`, `strid`, `katfgr` and corresponding name columns have not valuable information to forecast. This 3 columns are same

for all rows. Column grbname shows that all rows are revenues, strname and katfgrname – tax revenues. Column klsfpgr shows **7 type of taxes**, pklabp – **16 types of taxes**, spkprg – **252 types of taxes**. Columns pprg and spk are empty columns, ideally, they are used for not revenues, but for budget expenditures. It means that this hierarchy has only 4 levels.

**Second hierarchy** is administrative-territorial. As written above it has 4 levels. Initially, table does not have every level as distinct column, but it can be easily decomposed. First republican level has only 1 object, second regional level – 20 objects, third district level – 236, fourth rural level – 2694.

### *Preprocessing*

Dataset is high-quality, but it has few empty data. It has not 4 katonames for kato 616500000, 616600000, 616700000, 616800000. I wanted to find it, but there is no information in official reference books. Fortunately, it does not effect to forecast.

Another important dimension of this study is Kazakhstan's administrative-territorial decentralization. In 2022 the country reconfigured its regional map, creating three new oblasts – Abai, Zhetisu, and Ulytau – by presidential decree that entered into force on 7 June 2022 [5, 6]. The new regions were assembled from entire districts and cities transferred, respectively, from East Kazakhstan, Almaty, and Karaganda, without splitting lower-level units [5]. To operationalize the reform, the Government approved an action plan in June 2022 to define borders, establish territorial bodies, and staff the new administrations [7]. For fiscal analysis, this timing matters: separate oblast budgets for Abai, Zhetisu, and Ulytau were adopted by regional maslikhats in mid-December 2022 and took effect on 1 January 2023, making 2023 the first full fiscal year with standalone budgeting for these regions [8, 9, 10]. Accordingly, empirical series that cross 2022 should be reconciled to the post-reform administrative map to avoid structural breaks in regional aggregates.

Rural settlements which located in these districts are have same kato only first 4 digits are changed.

Another preprocessing step is with tax amount. Data in sumrg column is cumulative for every year. It means that for every month there are sum of tax amount from January to this month. To make forecasting better it is necessary to find value for every month. It is simple – just finding difference for consequent months (except January).

**Models.** There are described 2 type of models: Exponential smoothing and ARIMA. This section gives not only formulas and theoretical background, but also evolution of this models from initial idea and simple model to complex ones.

### *Exponential Smoothing*

Exponential smoothing is a time series forecasting method for univariate data that can be extended to support data with a trend or seasonal component. It was first proposed by Robert G. Brown in the 1950s and later generalized by Charles Holt and Peter Winters. Exponential smoothing techniques are particularly effective for short-term forecasting and are widely used in fields such as economics, inventory control, and demand forecasting [11].

The core idea of exponential smoothing is to forecast future values by combining past observations in a weighted manner, where the weights decrease exponentially as observations get older. This makes it responsive to recent changes in the data while still considering historical values. There are several variations of exponential smoothing, including simple exponential smoothing, Holt's linear trend method, and Holt-Winters' seasonal method [3]. But only the last one is used.

**Holt-Winters' Seasonal Method:** This method extends Holt's approach by adding a seasonal component, suitable for time series with both trend and seasonality. It comes in two forms – additive and multiplicative – depending on the nature of the seasonal fluctuations.

Additive (season):

$$L_t = \alpha * (Y_t - S_{t-s}) + (1 - \alpha) * (L_{t-1} + T_{t-1})$$

$$T_t = \beta * (L_t - L_{t-1}) + (1 - \beta) * T_{t-1}$$

$$S_t = \gamma * (Y_t - L_t) + (1 - \gamma) * S_{t-s}$$

$$F_{t+m} = L_t + m * T_t + S_{t-s+m}$$

Multiplicative (season):

$$L_t = \alpha * (Y_t / S_{t-s}) + (1 - \alpha) * (L_{t-1} + T_{t-1})$$

$$T_t = \beta * (L_t - L_{t-1}) + (1 - \beta) * T_{t-1}$$

$$S_t = \gamma * (Y_t / L_t) + (1 - \gamma) * S_{t-s}$$

$$F_{t+m} = (L_t + m * T_t) * S_{t-s+m}$$

where  $S_t$  is seasonal value,  $s$  is length of seasonal period and  $\gamma$  is seasonal smoothing.

Holt-Winters is powerful for complex series but involves more parameters ( $\alpha$ ,  $\beta$ ,  $\gamma$ ) that must be tuned carefully. It is widely used in business and economics for forecasting seasonal trends.

### SARIMA

ARIMA (Autoregressive Integrated Moving Average) is a classical statistical framework for modeling and forecasting univariate time series. The main intuition is that a time series can often be explained by two mechanisms: dependence on its own past values and dependence on past random shocks (errors). However, these linear dependence patterns are most stable and interpretable when the series is approximately stationary. Because many real-world economic and administrative time series contain trend and seasonality, ARIMA models typically begin with transformations – especially differencing – to remove non-stationary components. This approach is formalized in the Box–Jenkins methodology, which provides a structured workflow for identification, estimation, diagnostic checking, and forecasting [12, 13, 3].

The key generalization is **ARIMA(p, d, q)**, where the “I” (Integrated) indicates that the series is differenced ( $d$ ) times to achieve stationarity before applying an ARMA model. The first difference is defined as:

$$\nabla y_t = y_t - y_{t-1}$$

and applying differencing  $d$  times yields  $\nabla^d y_t$ . The ARIMA model can be written as an ARMA model on the differenced series:

$$y_t = c + \sum_{i=1}^p \phi_i \nabla^d y_{t-i} + \varepsilon_t + \sum_{j=1}^q \theta_j \varepsilon_{t-j}$$

Here,  $p$  controls how many lagged values influence the differenced series,  $d$  controls the degree of differencing, and  $q$  controls how many lagged errors influence the current value. In practice, the model orders are selected based on a combination of autocorrelation diagnostics, information criteria (such as AIC/AIC<sub>c</sub>/BIC), and residual checks.

For monthly datasets, seasonal behavior is common, and ARIMA is extended to **Seasonal ARIMA (SARIMA)**. SARIMA incorporates explicit seasonal differencing and seasonal AR/MA components, allowing the model to represent repeating patterns with period ( $s$ ) (for monthly data, typically  $s=12$ ). Seasonal differencing is defined as:

$$\nabla_s y_t = y_t - y_{t-s}$$

A SARIMA model is written as SARIMA( $p, d, q$ )( $P, D, Q$ ) $_s$ , where ( $P, D, Q$ ) are the seasonal counterparts of ( $p, d, q$ ), and  $D$  denotes the number of seasonal differences. The overall idea is to remove both non-seasonal trend (via  $d$ ) and repeating seasonal structure (via  $D$ ), and then model the remaining dependence using non-seasonal and seasonal AR/MA terms. This makes SARIMA a strong classical baseline for economic and fiscal time series with yearly cycles.

## Reconciliation methods

When time series are organized in a hierarchy (for example, country  $\rightarrow$  region  $\rightarrow$  district, or total taxes  $\rightarrow$  tax types  $\rightarrow$  subtypes), forecasts can be generated at multiple aggregation levels. If each series is forecast independently, the resulting forecasts are often incoherent, meaning that lower-level forecasts do not sum exactly to the corresponding higher-level forecasts. Forecast reconciliation is a set of methods that transform a collection of base forecasts into a coherent set that respects the aggregation constraints while aiming to improve accuracy [14].

A common way to express the hierarchy is through a summing matrix. Let  $\mathbf{y}$  denote the vector of bottom-level series (the most disaggregated level), and let  $\mathbf{Y}$  denote the vector of all series in the hierarchy (including aggregates). Then the aggregation structure can be written as:

where  $\mathbf{S}$  is a fixed “summing” matrix that encodes how bottom-level components add up to form higher-level totals [14].

Suppose  $\hat{\mathbf{y}}$  are **base forecasts** produced for all nodes of the hierarchy (often using the same forecasting model class at each node). Reconciliation constructs **coherent forecasts**  $\tilde{\mathbf{y}}$  by enforcing the aggregation constraints. A general linear reconciliation form is:

$$\tilde{\mathbf{y}} = \mathbf{S}\mathbf{G}\hat{\mathbf{y}}$$

where  $\mathbf{G}$  is a reconciliation (projection) matrix that depends on the chosen method [15, 3].

Below are the main reconciliation strategies used in practice.

Bottom-up reconciliation forecasts only the bottom-level series first, and then aggregates them upward to obtain forecasts for all higher levels. In matrix terms, this corresponds to selecting the bottom-level forecasts and applying the summing matrix  $\mathbf{S}$ . The bottom-up approach is

conceptually simple and guarantees coherence by construction. It is often effective when bottom-level series have relatively strong signal and sufficient historical data; however, it can perform poorly when bottom-level series are very noisy, because noise propagates upward through aggregation [14].

Top-down reconciliation starts from forecasting the most aggregated series (the top level) and then distributes that forecast down the hierarchy using a set of proportions. These proportions can be fixed (based on historical average shares) or time-varying (based on more adaptive allocation schemes). Top-down methods can be robust when bottom-level data are sparse or very noisy, but their accuracy depends heavily on whether the chosen allocation proportions remain stable over time. In addition, because lower-level forecasts are derived from the top forecast rather than directly modeled, important local patterns can be missed (Athanasopoulos et al., 2023).

Middle-out reconciliation is a compromise between bottom-up and top-down. It first forecasts a selected intermediate level of the hierarchy (a “middle” level). Then, forecasts for levels above are obtained by aggregating upward (bottom-up from the middle level), while forecasts for levels below are obtained by disaggregating downward (top-down from the middle level). The motivation is to anchor forecasting at a level where data are less noisy than the bottom level but still retain more granularity than the top level. The key practical choice is selecting the middle level, which may depend on data availability and the forecasting objective [15].

MinT is a statistically principled reconciliation approach that treats reconciliation as an optimal linear combination problem. Instead of relying on a single level (as in BU/TD/MO), MinT starts from base forecasts at all levels and computes coherent forecasts that minimize the total variance of reconciliation errors (the “trace” of the forecast error covariance matrix). In the general reconciliation form, MinT chooses using an estimate of the covariance matrix of base forecast errors, producing a weighted least squares solution. Empirically and theoretically, MinT often outperforms traditional approaches because it uses information from all levels and accounts for differences in uncertainty across series [15, 14].

## Training and testing

Model training and evaluation were implemented using Nixtla’s **StatsForecast** and **HierarchicalForecast** libraries. The training set covered monthly observations from **2016–2023**, while the test set consisted of **12 months of 2024** ( $h=12$ ). ETS and ARIMA-family models were fitted on the 2016–2023 period and used to generate multi-step forecasts for 2024. To ensure hierarchical coherence, reconciliation was applied as a post-processing step using the **Bottom-Up** method, because it preserves **low-level dynamics** by forecasting the most disaggregated series first and then aggregating upward. Two separate reconciliations were trained and evaluated: one for the **tax (budget classification) hierarchy** and one for the **administrative-territorial hierarchy**, enabling coherent forecasts within each hierarchical structure.

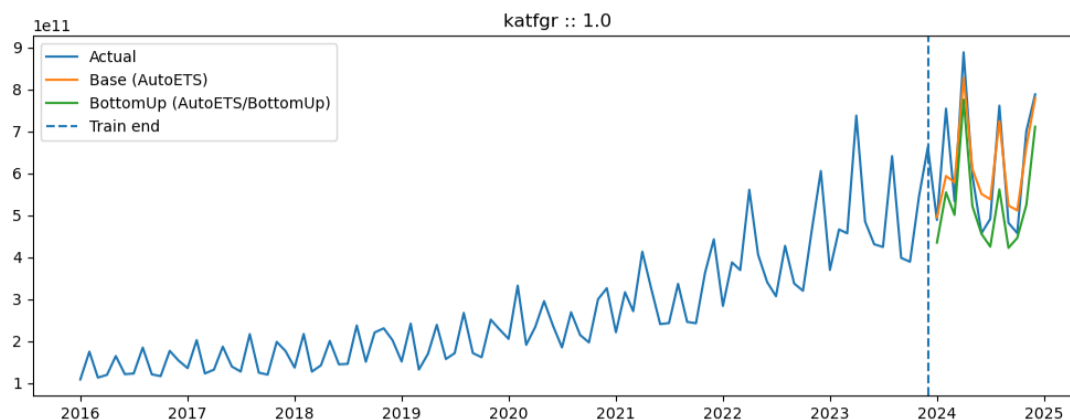
*Evaluation results for the tax (budget-classification) hierarchy*

| #  | Level                            | Metric       | AutoETS  | AutoARIMA | AutoETS<br>/BottomUp | AutoARIMA<br>/BottomUp |
|----|----------------------------------|--------------|----------|-----------|----------------------|------------------------|
| 0  | katfgr                           | mae-scaled   | 1.000000 | 0.919004  | 1.745084             | 1.092404               |
| 1  | katfgr                           | rmse-scaled  | 1.000000 | 1.035845  | 1.707657             | 1.150973               |
| 2  | katfgr                           | smape-scaled | 1.000000 | 0.891377  | 1.716222             | 1.038966               |
| 3  | katfgr/klsfpgr                   | mae-scaled   | 1.000000 | 0.621455  | 0.943973             | 0.686577               |
| 4  | katfgr/klsfpgr                   | rmse-scaled  | 1.000000 | 0.670378  | 0.880870             | 0.714426               |
| 5  | katfgr/klsfpgr                   | smape-scaled | 1.000000 | 0.763520  | 0.998946             | 0.808731               |
| 6  | katfgr/klsfpgr/<br>pklabp        | mae-scaled   | 1.000000 | 0.686506  | 1.066024             | 0.728571               |
| 7  | katfgr/klsfpgr/<br>pklabp        | rmse-scaled  | 1.000000 | 0.764334  | 1.039909             | 0.804596               |
| 8  | katfgr/klsfpgr/<br>pklabp        | smape-scaled | 1.000000 | 0.876702  | 1.026466             | 0.860148               |
| 9  | katfgr/klsfpgr/<br>pklabp/spkprg | mae-scaled   | 1.000000 | 0.701782  | 1.000000             | 0.701782               |
| 10 | katfgr/klsfpgr/<br>pklabp/spkprg | rmse-scaled  | 1.000000 | 0.765077  | 1.000000             | 0.765077               |
| 11 | katfgr/klsfpgr/<br>pklabp/spkprg | smape-scaled | 1.000000 | 0.959032  | 1.000000             | 0.959032               |
| 12 | Overall                          | mae-scaled   | 1.000000 | 0.702848  | 1.096031             | 0.753724               |
| 13 | Overall                          | rmse-scaled  | 1.000000 | 0.770659  | 1.060916             | 0.807255               |
| 14 | Overall                          | smape-scaled | 1.000000 | 0.919367  | 1.009230             | 0.920326               |

Table reports scaled accuracy metrics for the budget-classification hierarchy. In this evaluation, AutoETS is used as the benchmark, therefore its values are equal to 1.0, and the remaining results are expressed relative to AutoETS. Consequently, values below 1.0 indicate improvement over AutoETS, while values above 1.0 indicate worse performance. The comparison is provided for two base models (AutoETS and AutoARIMA) and their reconciled versions using Bottom-Up (AutoETS/BottomUp and AutoARIMA/BottomUp).

The results show a clear advantage of AutoARIMA over AutoETS when models are evaluated without reconciliation. In practical terms, this suggests that the budget-classification time series contain dependence structures (lags and shock propagation) that are better represented by ARIMA-type models than by exponential smoothing alone, especially once differencing and seasonality handling are applied.

When Bottom-Up reconciliation is applied, the evaluation indicates that coherence is achieved at the cost of accuracy, particularly for aggregated nodes. The overall metrics confirm that Bottom-Up does not improve accuracy in this hierarchy. Therefore, even though Bottom-Up produces coherent forecasts, it does not lead to better average predictive accuracy for this particular hierarchy and split.



A more detailed look across levels explains why this happens. At the top level (katfgr) reconciliation strongly degrades performance for both model families (line chart above shows it visually), and especially for AutoETS: AutoETS/BottomUp reaches extremely high scaled errors (approximately 1.71–1.75 across metrics), meaning the coherent top forecast produced by aggregating noisy lower-level predictions is substantially worse than the direct top-level ETS forecast. AutoARIMA/BottomUp is also worse than AutoARIMA at the top level (e.g., MAE-scaled increases from 0.9190 to 1.0924), although the deterioration is not as dramatic as for ETS. This behavior is consistent with a known property of Bottom-Up: the top-level forecast becomes the sum of many bottom-level forecasts, and any noise, local irregularities, or model misspecification at low levels accumulates upward, which can harm aggregated accuracy when bottom series are volatile.

Overall, the evaluation supports two main conclusions for the budget-classification hierarchy. First, AutoARIMA is the best-performing approach among the compared options, delivering the lowest overall errors across MAE, RMSE, and sMAPE. Second, Bottom-Up reconciliation is useful primarily for enforcing hierarchical coherence and preserving low-level dynamics, but in this hierarchy it introduces an accuracy penalty at aggregated levels, which leads to worse overall results than the best unreconciled model. This trade-off is important for interpretation in applied settings: if coherent forecasts are required for reporting and budgeting constraints, Bottom-Up provides a consistent system of forecasts, but if the primary objective is minimizing forecast error at higher aggregation levels, unreconciled AutoARIMA (or more statistically efficient reconciliation methods such as MinT) may be preferable.

### *Evaluation results for the administrative-territorial hierarchy*

| # | Level           | Metric       | AutoETS  | AutoARIMA | AutoETS /BottomUp | AutoARIMA /BottomUp |
|---|-----------------|--------------|----------|-----------|-------------------|---------------------|
| 0 | Republic        | mae-scaled   | 1.000000 | 1.176773  | 1.359108          | 1.200653            |
| 1 | Republic        | rmse-scaled  | 1.000000 | 1.285107  | 1.459671          | 1.281778            |
| 2 | Republic        | smape-scaled | 1.000000 | 1.091405  | 1.199854          | 1.103488            |
| 3 | Republic/Region | mae-scaled   | 1.000000 | 0.885138  | 0.967459          | 0.899431            |
| 4 | Republic/Region | rmse-scaled  | 1.000000 | 0.817277  | 0.955003          | 0.844261            |
| 5 | Republic/Region | smape-scaled | 1.000000 | 0.854601  | 0.913037          | 0.881310            |

|    |                               |              |          |          |          |          |
|----|-------------------------------|--------------|----------|----------|----------|----------|
| 6  | Republic/Region/District      | mae-scaled   | 1.000000 | 0.978699 | 0.992699 | 0.976654 |
| 7  | Republic/Region/District      | rmse-scaled  | 1.000000 | 0.960116 | 0.995975 | 0.960185 |
| 8  | Republic/Region/District      | smape-scaled | 1.000000 | 0.936663 | 0.964351 | 0.931937 |
| 9  | Republic/Region/District/kato | mae-scaled   | 1.000000 | 0.987494 | 1.000000 | 0.987494 |
| 10 | Republic/Region/District/kato | rmse-scaled  | 1.000000 | 0.965390 | 1.000000 | 0.965390 |
| 11 | Republic/Region/District/kato | smape-scaled | 1.000000 | 0.949395 | 1.000000 | 0.949395 |
| 12 | Overall                       | mae-scaled   | 1.000000 | 0.983247 | 1.033888 | 0.988976 |
| 13 | Overall                       | rmse-scaled  | 1.000000 | 0.962354 | 1.037498 | 0.968558 |
| 14 | Overall                       | smape-scaled | 1.000000 | 0.948106 | 0.996900 | 0.947805 |

In contrast to the budget-classification hierarchy – where AutoARIMA strongly dominated AutoETS at almost every level – the administrative-territorial hierarchy shows a more mixed pattern. At the top node (Republic), AutoARIMA performs worse than AutoETS across all metrics (MAE 1.1768, RMSE 1.2851, sMAPE 1.0914). This indicates that, at the most aggregated national level, the series is likely smoother and better represented by level/trend dynamics captured by ETS, while ARIMA's differencing/lag structure does not provide an advantage.

However, beginning from the Region level and below, AutoARIMA becomes consistently better than AutoETS (values below 1.0). The improvements are especially visible at the Region level (e.g., RMSE-scaled 0.8173 and sMAPE-scaled 0.8546), and remain present – although smaller – at District and KATO levels. This suggests that once the national series is decomposed into geographic components, local dynamics and autocorrelation patterns become more important, and ARIMA benefits from modeling lag dependence and seasonal behavior.

At the overall line, AutoARIMA is slightly better than AutoETS for all metrics (Overall MAE 0.9832, RMSE 0.9624, sMAPE 0.9481). Compared to the budget hierarchy, these gains are modest, meaning that the administrative-territorial hierarchy is not a setting where ARIMA dramatically outperforms ETS; instead, performance depends on the aggregation level.

Bottom-Up reconciliation again guarantees coherence by constructing higher-level forecasts as sums of bottom-level forecasts. In this hierarchy, the effect is more stable than in the budget-classification hierarchy, but it still introduces a clear trade-off.

For AutoETS, Bottom-Up slightly worsens the overall results (Overall MAE increases from 1.0000 to 1.0339 and RMSE from 1.0000 to 1.0375), while sMAPE remains almost unchanged (0.9969). For AutoARIMA, Bottom-Up has only a small negative impact on MAE and RMSE (Overall MAE 0.98898 vs 0.98325; RMSE 0.96856 vs 0.96235), and is essentially neutral for sMAPE (0.9478 vs 0.9481). This is notably different from the budget hierarchy, where

Bottom-Up produced a stronger deterioration at aggregated levels and a more visible overall penalty.

At the top node, Bottom-Up worsens performance for both model families, and the deterioration is substantial for the Republic series (e.g., AutoETS increases from 1.0 to 1.3591 MAE-scaled, and AutoARIMA increases from 1.1768 to 1.2007). This is consistent with Bottom-Up behavior: the national forecast becomes an aggregation of many lower-level forecasts, so noise or local errors can accumulate upward. At the bottom level (KATO), Bottom-Up does not change the AutoARIMA values and sets AutoETS/BottomUp to 1.0, reflecting that Bottom-Up reconciliation is anchored on bottom-level series.

When comparing the two hierarchies under the same evaluation setup (same benchmark scaling, same models, same Bottom-Up reconciler), a consistent difference emerges. The budget-classification hierarchy exhibits stronger gains from AutoARIMA at the base-forecast stage, but also a larger accuracy penalty after Bottom-Up reconciliation, particularly at the most aggregated node. In contrast, the administrative-territorial hierarchy shows smaller differences between ETS and ARIMA overall and a more stable reconciliation behavior, where Bottom-Up is closer to neutral for percentage-based error (sMAPE) and introduces only a small overall degradation for ARIMA.

Therefore, if “better hierarchical forecasting” is understood as producing coherent forecasts with minimal loss of accuracy, then the administrative-territorial hierarchy performs better: Bottom-Up is less damaging and results are more consistent across levels. If “better” is understood as the maximum achievable accuracy using the best base model before reconciliation, then the budget-classification hierarchy favors AutoARIMA more strongly, but that advantage is reduced when strict coherence is enforced via Bottom-Up.

**Conclusion.** This study investigated short-term forecasting of Kazakhstan’s tax revenues using official monthly data from the E-MinFin (Ministry of Finance) API for January 2016–May 2025. The dataset exhibits a grouped structure with two independent hierarchies: (i) budget classification (tax-type hierarchy) and (ii) administrative-territorial structure (Republic → Region → District → KATO). After preprocessing [7], classical statistical forecasting models were trained and evaluated in a consistent backtesting setup (train: 2016–2023; test: 2024; horizon: 12 months) using Nixtla’s StatsForecast and HierarchicalForecast tooling.

Across both hierarchies, unreconciled AutoARIMA generally delivered stronger accuracy than AutoETS, indicating that lagged dependence and seasonal differencing capture important dynamics in Kazakhstan’s tax revenue series – especially in the budget-classification hierarchy. However, model performance was strongly level-dependent in the administrative-territorial hierarchy: at the national (Republic) aggregate, ETS outperformed ARIMA, while ARIMA became consistently preferable at regional and lower levels. These findings imply that no single model class dominates uniformly across aggregation levels; model choice should be conditional on the target reporting level and its signal-to-noise characteristics.

To enforce coherence, Bottom-Up reconciliation was applied separately within each hierarchy. The results show a clear accuracy–coherence trade-off: Bottom-Up guarantees additivity but can degrade accuracy at higher aggregation levels due to error accumulation from

many noisy bottom-level forecasts. This effect was pronounced in the budget-classification hierarchy (notably at the top node), where reconciliation introduced a substantial penalty relative to the best unreconciled approach. In the administrative-territorial hierarchy, Bottom-Up was comparatively more stable and close to neutral in percentage-based error (sMAPE) for ARIMA, though still harmful at the top aggregate. Practically, this indicates that Bottom-Up is suitable when coherent lower-level signals are essential for operational planning, but it may be suboptimal when accuracy at the most aggregated levels is the primary objective.

From an applied public-finance perspective, the study contributes (1) a reproducible forecasting pipeline tailored to Kazakhstan's institutional data structures, (2) evidence that ARIMA-family approaches remain highly competitive for short-horizon fiscal forecasting on short monthly histories, and (3) an empirical demonstration that reconciliation strategy materially affects performance and should be selected based on the decision level (national vs. regional vs. granular).

Key limitations include the relatively short time span (117 monthly observations), the univariate modeling setup (tax amount only), and the use of a single reconciler (Bottom-Up). Future work should evaluate statistically efficient reconciliation (e.g., MinT), incorporate exogenous macroeconomic or commodity-price indicators, and explore global/ML models that share information across related series (e.g., embeddings across tax categories or regions) to improve robustness under structural breaks and data sparsity – especially at the most disaggregated levels.

### References:

1. Lahiri K., Yang, C. Boosting tax revenues with mixed-frequency data in the aftermath of COVID-19: The case of New York (CESifo Working Paper No. 9365). SSRN. – 2021. URL: <https://ssrn.com/abstract=3950100>
2. Karmy J. P., Maldonado, S. Hierarchical time series forecasting via support vector regression in the European travel retail industry. *Expert Systems with Applications*, 137, 59–73. – 2019. URL: <https://doi.org/10.1016/j.eswa.2019.06.060>
3. Hyndman R. J., Athanasopoulos, G. *Forecasting: Principles and practice* (2nd ed.). – OTexts, 2018.
4. Serikova M., Sembiyeva L., Balginova K., Alina G., Shakharova A., Kurmanalina, A. Tax revenues estimation and forecast for state tax audit // *Entrepreneurship and Sustainability Issues*. – 2020. – T. 7, № 3. – C. 2419–2435. – DOI: [https://doi.org/10.9770/jesi.2020.7.3\(64\)](https://doi.org/10.9770/jesi.2020.7.3(64)).
5. President of the Republic of Kazakhstan. O nekotorykh voprosakh administrativno-territorial'nogo ustroystva Respubliki Kazakhstan [On some issues of the administrative-territorial structure of the Republic of Kazakhstan] (Decree No. 887). Adilet Legal Information System. – 2022a. URL: <https://adilet.zan.kz/rus/docs/U2200000887>
6. President of the Republic of Kazakhstan. O nekotorykh voprosakh administrativno-territorial'nogo ustroystva Respubliki Kazakhstan [On some issues of the administrative-territorial structure of the Republic of Kazakhstan] (Press release). Official website of the President (Akorda). – 2022b. URL: <https://www.akorda.kz/ru/o-nekotorykh-voprosakh-administrativno-territorialnogo-ustroystva-respubliki-kazahstan-445923>
7. Prime Minister of the Republic of Kazakhstan. Pravitel'stvom utverzhden plan meropriyatii po ustroistvu oblastei Abai, Zhetisu i Ulytau [The Government approved the action plan to set up the Abai, Zhetisu and Ulytau regions]. – 2022. URL:

<https://primeminister.kz/ru/news/pravitelstvom-utverzhdenn-plan-meropriyatiy-po-ustroystvu-oblastey-abay-zhetisu-i-ulytau-352044>

8. Maslikhat of Abai Region. Ob oblastnom byudzhete na 2023–2025 gody [On the oblast budget for 2023–2025] (Decision No. 11/66-VII). Adilet Legal Information System. – 2022. URL: <https://adilet.zan.kz/rus/docs/G22F001166M>

9. Maslikhat of Zhetisu Region. Ob oblastnom byudzhete oblasti Zhetisu na 2023–2025 gody [On the Zhetisu oblast budget for 2023–2025] (Decision No. 13-39). Adilet Legal Information System. – 2022. URL: <https://adilet.zan.kz/rus/docs/G22I001339M>

10. Maslikhat of Ulytau Region. Ob oblastnom byudzhete na 2023–2025 gody [On the oblast budget for 2023–2025] (Decision No. 12/84). Adilet Legal Information System. – 2022. URL: <https://adilet.zan.kz/rus/docs/G22H001284M>

11. Brown R. G. Statistical forecasting for inventory control. – McGraw-Hill, 1959.

12. Box G. E. P., Jenkins G. M. Time series analysis: Forecasting and control. – Holden-Day, 1970.

13. Box G. E. P., Jenkins G. M., Reinsel G. C., Ljung G. M. Time series analysis: Forecasting and control (5th ed.). – John Wiley & Sons, 2015.

14. Hyndman R. J., Ahmed R. A., Athanasopoulos G., Shang H. L. Optimal combination forecasts for hierarchical time series // Computational Statistics & Data Analysis. – 2011. – T. 55, № 9. – С. 2579–2589.

15. Wickramasuriya S. L., Athanasopoulos G., Hyndman R. J. Optimal forecast reconciliation for hierarchical and grouped time series through trace minimization // Journal of the American Statistical Association. – 2019. – T. 114, № 526. – С. 804–819. – DOI: <https://doi.org/10.1080/01621459.2018.1448825>.

16. Mancuso P., Piccialli V., Sudoso A. M. A machine learning approach for forecasting hierarchical time series. Expert Systems with Applications, 182, 115102. – 2021. URL: <https://doi.org/10.1016/j.eswa.2021.115102>

17. Wickramasuriya S. L., Athanasopoulos G., Hyndman R. J. Optimal forecast reconciliation for hierarchical and grouped time series through trace minimization. Journal of the American Statistical Association. – 2018. URL: <https://doi.org/10.1080/01621459.2018.1448825>

18. Khorasani Buxton E., Kriz K. A., Cremeens M., Jay, K. An auto regressive deep learning model for sales tax forecasting from multiple short time series // Proceedings of the 2019 18th IEEE International Conference on Machine Learning and Applications (ICMLA) (pp. 1359–1364). – 2019. – DOI: <https://doi.org/10.1109/ICMLA.2019.00221>.

УДК 347.1

**Balmakhanov Danial Talgatuly,****Aldashev Aslan Kanatovich**

2<sup>nd</sup> years students  
«Software Engineering» EP  
Astana IT University  
(Astana, Kazakhstan)

**Osserbay Amandos Nurboluly**

2<sup>nd</sup> years student  
«Cybersecurity» EP  
Astana IT University  
(Astana, Kazakhstan)

## **DEVELOPMENT AND EVALUATION OF AN AI-BASED INTRUSION DETECTION SYSTEM FOR NETWORK TRAFFIC**

**Abstract:** This study presents the development and systematic evaluation of an AI-based intrusion detection system (IDS) for network traffic classification with a particular focus on robustness under temporal distribution shift. While many existing studies report near-perfect performance using random train–test splits, such evaluation schemes often fail to reflect realistic deployment conditions in dynamic network environments.

The experiments were conducted using the CICIDS2017 dataset. Two ensemble learning models, Random Forest and XGBoost, were implemented and evaluated under both in-domain and cross-session scenarios. In the in-domain setting (Wednesday → Wednesday), both models achieved near-perfect performance, with accuracy exceeding 99.9% and attack recall above 0.999.

However, under cross-session evaluation (Wednesday → Friday), a significant performance degradation was observed. Random Forest achieved approximately 79% accuracy with attack recall around 0.63, while XGBoost demonstrated similar degradation despite maintaining high ROC-AUC values. A training-size ablation study showed that increasing the volume of training data did not substantially improve cross-session recall, indicating that distribution shift rather than data scarcity is the primary limiting factor.

A Kolmogorov–Smirnov statistical analysis confirmed substantial feature distribution differences between sessions. Additionally, threshold sensitivity experiments demonstrated the trade-off between recall and false positive rate under deployment constraints.

The results highlight the critical importance of cross-session validation when evaluating AI-based intrusion detection systems. Although ensemble models perform exceptionally well under controlled conditions, achieving stable generalization in evolving network environments remains a significant challenge.

**Keywords:** Intrusion Detection System (IDS), Machine Learning, Random Forest, XGBoost, Distribution Shift, Cross-Session Evaluation, Network Traffic Analysis, Covariate Shift, Robustness, Threshold Analysis

Intrusion Detection Systems (IDS) were introduced to address the growing complexity of cyber threats and the limitations of perimeter-based security mechanisms such as firewalls. Early network defense strategies relied primarily on static filtering and rule-based monitoring, which proved insufficient as attack techniques evolved. IDS are typically categorized into two primary types: signature-based systems and anomaly-based systems. Signature-based IDS detect malicious activity by matching network traffic patterns against a database of known attack signatures. These systems are effective against previously identified threats and widely used in commercial products. However, they suffer from significant limitations. First, they cannot detect zero-day attacks, as no signature exists for unknown threats. Second, attackers can modify payloads or use obfuscation techniques to bypass static pattern matching.

Third, maintaining large signature databases requires continuous manual updates. Anomaly-based IDS were proposed to overcome these weaknesses. Instead of relying on predefined signatures, anomaly-based systems establish a model of normal behavior and classify deviations as potential intrusions. This approach enables detection of previously unseen attacks.

However, anomaly detection introduces new challenges, particularly high false positive rates due to natural variability in legitimate network traffic. The integration of Artificial Intelligence (AI) and Machine Learning (ML) techniques into anomaly-based IDS has significantly enhanced their capability to model complex traffic patterns. ML-based IDS can process high-dimensional flow-based features and automatically learn decision boundaries separating benign and malicious traffic.

To assess robustness under distribution shift, models trained on Wednesday traffic were evaluated on Friday traffic.

Under this cross-session setting, performance degraded significantly.

Random Forest achieved:

- Accuracy: 79%
- Recall (Attack): 0.64
- F1-score (Attack): 0.78

XGBoost achieved:

- Accuracy: 77%
- Recall (Attack): 0.60
- F1-score (Attack): 0.75

Although precision for the attack class remained high (close to 1.0), recall decreased substantially. This indicates that while the models rarely misclassify benign traffic as malicious, they fail to detect a considerable portion of attacks under cross-day conditions.

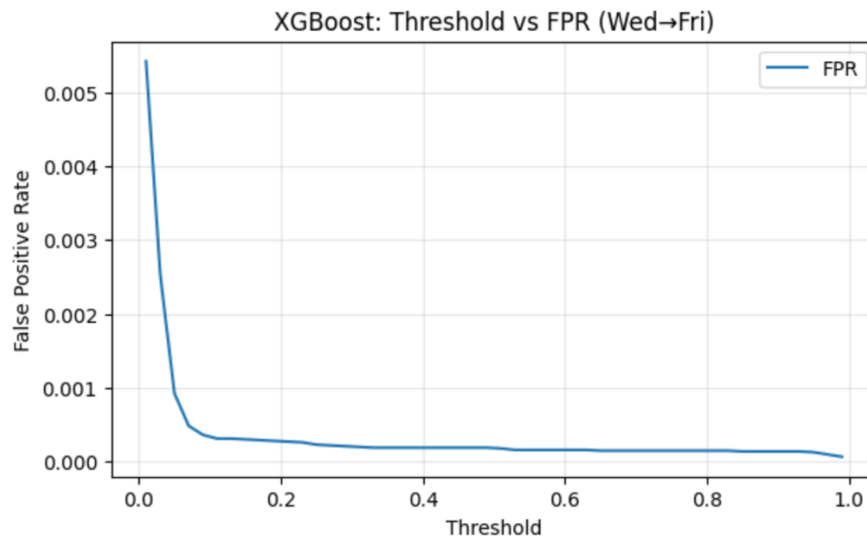


Fig - 1. Impact of classification threshold on False Positive Rate for XGBoost

As shown in Figure 1, FPR rapidly decreases as the threshold increases, remaining below 0.001 for thresholds above 0.05.

To further investigate cross-session degradation, threshold optimization was performed on the Friday dataset. Although ROC-AUC remained high (0.995), the default classification threshold (0.5) resulted in suboptimal recall for the attack class.

By adjusting the threshold, different operating regimes were obtained:

- At threshold = 0.5 (default), Recall = 0.627, FPR = 0.00017
- At threshold = 0.05 (FPR  $\leq$  0.001 constraint), Recall = 0.635
- At threshold = 0.01 (maximum F1), Recall = 0.665, FPR = 0.0054

These results demonstrate that the model retains strong ranking capability under distribution shift. The degradation observed under cross-day evaluation is partially attributable to threshold miscalibration rather than complete loss of discriminative power.

This finding highlights the importance of operating point selection in real-world intrusion detection systems, where recall–FPR trade-offs must be carefully controlled.

The experimental results clearly demonstrate a critical distinction between in-domain performance and real-world robustness. Under same-session evaluation, both Random Forest and XGBoost achieved near-perfect classification metrics. Such results are consistent with many previously published studies reporting accuracy values exceeding 99% on benchmark datasets.

However, these results may create a misleading perception of model reliability. In-domain evaluation assumes that training and testing data are drawn from identical distributions. While this assumption simplifies benchmarking, it does not reflect operational environments where traffic patterns evolve over time.

The near-saturation performance observed even with only 10% of the training data further indicates that Wednesday traffic patterns are relatively easy to model under static conditions. This suggests that high in-domain accuracy does not necessarily imply model robustness.

The cross-day experiments reveal a substantial degradation in performance when models trained on Wednesday data are evaluated on Friday traffic. Despite high precision, recall for the attack class decreases significantly, indicating that a considerable portion of malicious traffic remains undetected.

The training-size ablation study provides additional insight. Increasing the volume of Wednesday training data from 10% to 100% did not

meaningfully improve cross-day performance. This observation strongly suggests that insufficient training data is not the primary cause of performance degradation.

Instead, the results point to distribution shift as the dominant limiting factor. Differences in feature distributions, attack patterns, and traffic dynamics between Wednesday and Friday sessions likely alter the learned decision boundaries, reducing model effectiveness.

Although the cross-day ROC-AUC remains high (above 0.96 for both models), the recall for the attack class significantly decreases. This apparent contradiction can be explained by the difference between ranking-based and threshold-based evaluation metrics. ROC-AUC measures the model's ability to correctly rank positive instances above negative ones, independently of a specific classification threshold. In contrast, recall depends directly on the chosen decision threshold (typically 0.5). Under distribution shift, the predicted probability distribution shifts, leading to suboptimal threshold calibration. Therefore, while the models preserve strong discriminative ranking ability, the default threshold fails to capture a substantial portion of malicious traffic.

This finding aligns with broader machine learning theory, which emphasizes the importance of distribution alignment for reliable generalization.

### References:

1. D. E. Denning, "An Intrusion-Detection Model," IEEE Transactions on Software Engineering, vol. SE-13, no. 2, pp. 222–232, 1987.
2. K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94, 2007.
3. M. Tavallaei, E. Bagheri, W. Lu, and A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," in Proc. IEEE Symposium on Computational Intelligence for Security and Defense Applications, 2009.
4. I. Sharafaldin, A. Lashkari, and A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in Proc. ICISSP, 2018.
5. M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A Survey of Network-Based Intrusion Detection Data Sets," Computers & Security, vol. 86, pp. 147–167, 2019.
6. L. Breiman, "Random Forests," Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.

УДК 14.00.00

**Жигер Емжаев**

студент-магистрант

направления «Гигиена и охрана труда на производстве»

Казахский национальный исследовательский

технический университет имени К.И.Сатпаева

(г. Алматы, Казахстан)

## **ВНЕДРЕНИЕ МОДУЛЬНОЙ СИСТЕМЫ ОБУЧЕНИЯ РАБОЧЕГО ПЕРСОНАЛА В УСЛОВИЯХ КРУПНОЙ ПРОМЫШЛЕННОЙ ОРГАНИЗАЦИИ: ФАКТОРЫ ЭФФЕКТИВНОСТИ И ОРГАНИЗАЦИОННЫЕ РИСКИ**

**Аннотация:** В статье представлены результаты педагогического исследования эффективности внедрения модульной системы обучения рабочего персонала в условиях крупного промышленного предприятия уранодобывающей отрасли. Исследование проведено на двух производственных площадках (рудники X и Y). Общая численность работников предприятия составляет 3000–3500 человек, в анкетировании приняли участие 150 сотрудников различных профессиональных категорий. Для анализа взаимосвязей между факторами внедрения и результатами обучения использована модель структурных уравнений (PLS-SEM). Результаты подтверждают положительное влияние модульного обучения на вовлечённость персонала, перенос знаний в практическую деятельность и укрепление культуры безопасности. Одновременно выявлены организационные ограничения и риски формализации процесса обучения.

**Ключевые слова:** модульное обучение, промышленная безопасность, культура безопасности, вовлеченность персонала, перенос обучения, PLS-SEM.

Крупные предприятия уранодобывающей отрасли функционируют в условиях повышенной технологической сложности и производственных рисков. В подобных условиях устойчивость системы промышленной безопасности напрямую зависит от качества подготовки рабочего персонала.

Исследования в сфере электронного обучения показывают, что цифровые форматы подготовки не всегда обеспечивают устойчивый перенос знаний в практическую деятельность и могут приводить к формальному прохождению курсов без изменения поведения работников [3]. Это требует поиска педагогических решений, способных обеспечить формирование устойчивых моделей безопасного поведения.

Модульная система обучения рассматривается как инструмент структурирования образовательного процесса в виде автономных компетентностных блоков, адаптируемых к изменениям производственных требований [1]. Такой подход особенно актуален в условиях динамических технологических изменений и необходимости регулярного обновления компетенций персонала [1].

Существенную роль играет релевантность содержания обучающих модулей реальным производственным рискам. Недостаточная связь теоретического материала с практикой снижает воспринимаемую полезность обучения и уровень вовлеченности работников [2]. Кроме того, цифровая реализация модулей усиливает образовательный эффект лишь при грамотном методическом проектировании и организационной поддержке внедрения [4].

Таким образом, актуальность исследования обусловлена необходимостью педагогической оценки эффективности внедрения модульной системы обучения в условиях крупного промышленного предприятия.

Модульная архитектура обучения позволяет формировать систему управляемых компетенций, обеспечивая гибкость обновления образовательного контента в соответствии с изменениями производственных процессов [1]. В условиях промышленной среды это особенно важно при наличии различных профессиональных категорий и уровней допуска к работам.

Релевантность содержания выступает ключевым фактором результативности обучения. Ориентация модулей на реальные производственные сценарии и типовые ошибки работников повышает степень усвоения материала и способствует формированию устойчивых навыков безопасной деятельности [2].

Цифровые формы обучения обеспечивают доступность и прозрачность образовательного процесса, однако при недостаточной интерактивности или перегруженности контентом возможно снижение вовлеченности персонала [3]. Следовательно, технологическое внедрение должно сопровождаться методическим контролем качества образовательных модулей [4].

Вовлеченность рассматривается как центральный механизм преобразования учебного воздействия в изменение профессионального поведения [4]. Перенос обучения в практическую деятельность возможен лишь при интеграции образовательной системы в общую модель управления персоналом и наличии управленческой поддержки [5].

На основании анализа литературы сформирована концептуальная модель исследования, отражающая последовательную связь факторов внедрения и поведенческих результатов обучения.

### 3. Концептуальная модель исследования



Рисунок 1 – Концептуальная модель влияния факторов внедрения модульного обучения\

Структурная модель была построена методом PLS-SEM для оценки взаимосвязей между факторами внедрения, вовлечённостью, результативностью обучения, переносом знаний и безопасным поведением. Полученная модель подтвердила ключевые гипотезы исследования.

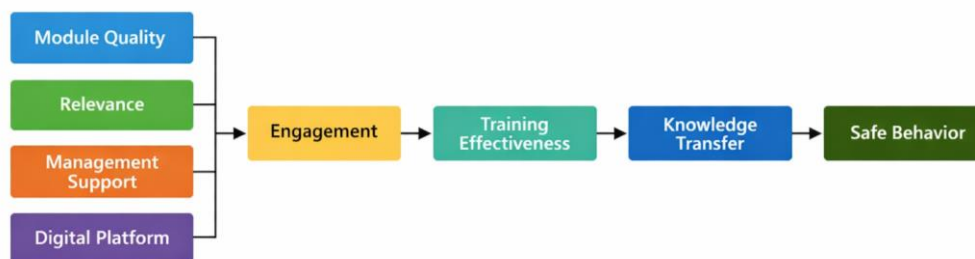


Рисунок 2 – Структурная модель *PLS-SEM*

Рисунок 2 – Структурная модель взаимосвязей (PLS-SEM)

Полученные данные позволяют выделить ключевые медиаторные механизмы: вовлечённость персонала и перенос знаний. Они являются звеньями, через которые образовательные воздействия превращаются в изменение реального поведения.



Рисунок 3 – Медиаторная роль вовлеченности и переноса обучения

Модульная система обучения способствует формированию культуры безопасности через последовательные этапы: обучение модульному контенту, осознание рисков, изменение установок, изменение поведения и закрепление безопасных практик. Этот механизм представлен на рисунке.



Рисунок 4 – Механизм формирования культуры безопасности

Исследование проведено на базе крупного промышленного предприятия уранодобывающей отрасли. Общая численность работников составляет 3000–3500 человек. В исследовании приняли участие 150 сотрудников двух производственных площадок (рудники X и Y), представляющих различные профессиональные группы: рабочие, инженерно-технический персонал, специалисты служб безопасности и административные сотрудники.

Анкетирование включало оценку таких показателей, как качество модульного дизайна, релевантность содержания, поддержка руководства, удобство цифровой платформы, вовлечённость работников, воспринимаемая эффективность обучения, перенос знаний в практику и соблюдение требований безопасности.

Для анализа данных использована модель структурных уравнений методом частичных наименьших квадратов (PLS-SEM), что позволяет исследовать сложные причинно-следственные связи между латентными переменными и медиаторные эффекты [4]. Этот метод широко применяется в исследованиях организационного обучения и промышленной безопасности [4].

Анализ измерительной модели подтвердил надежность и валидность используемых шкал. Показатели внутренней согласованности соответствовали общепринятым требованиям, а критерии конвергентной и дискриминантной валидности подтвердили корректность построения латентных переменных.

Структурная модель показала положительное влияние качества модульного дизайна и релевантности содержания на вовлечённость персонала. Данный результат согласуется с выводами о значимости структурированности и адаптивности модульных программ в производственной среде [1].

Вовлечённость продемонстрировала статистически значимое влияние на воспринимаемую эффективность обучения, что подтверждает положение о ключевой роли вовлечённости как механизма изменения профессионального поведения [4].

Эффективность обучения оказала положительное влияние на перенос знаний в практическую деятельность. Перенос, в свою очередь, показал значимую связь с соблюдением требований безопасности, что подтверждает необходимость оценки поведенческого эффекта обучения, а не только уровня знаний [3].

В целом результаты свидетельствуют о положительном педагогическом эффекте внедрения модульной системы обучения и ее вкладе в укрепление культуры безопасности предприятия.

Полученные данные подтверждают, что модульная структура обучения обеспечивает управляемость компетенций и способствует адаптации персонала к изменениям производственных процессов [1]. Существенная роль релевантности содержания согласуется с выводами о необходимости ориентации обучения на реальные производственные риски [2].

Выявленный медиаторный эффект вовлеченности подтверждает концепцию, согласно которой изменение поведения невозможно без внутренней включенности работника в образовательный процесс [4]. Цифровая составляющая обучения усиливает эффект при условии методической выверенности и организационной поддержки, что соответствует результатам исследований в сфере e-training [3].

Вместе с тем выявлены организационные ограничения внедрения модульного обучения: риск формального прохождения модулей без реального вовлечения, перегрузка образовательного контента, зависимость результата от качества методического проектирования и необходимость постоянной управленческой поддержки. Подобные ограничения отмечаются и в исследованиях цифровых образовательных технологий в промышленной среде [3; 4].

Несмотря на указанные риски, результаты исследования указывают на положительную динамику формирования культуры безопасности и повышение осознанности работников в вопросах соблюдения требований промышленной безопасности.

Внедрение модульной системы обучения в условиях крупного промышленного предприятия уранодобывающей отрасли демонстрирует положительный педагогический эффект. Эффективность обучения опосредуется вовлечённостью персонала и механизмом переноса знаний в практическую деятельность.

Модульная архитектура подготовки способствует укреплению культуры безопасности и повышению соблюдения требований промышленной безопасности. Устойчивость результата зависит от качества проектирования модулей, их релевантности производственным рискам и уровня организационной поддержки.

Ограничением исследования является анализ данных двух производственных площадок и использование самооценочных показателей. Дальнейшие исследования могут быть направлены на расширение выборки и интеграцию объективных производственных индикаторов.

#### **Список литературы:**

1. Zidi S., et al. Towards a Modular Approach for Workforce Qualification in Reconfigurable Manufacturing Systems. *Procedia Computer Science*, 2024.
2. Arif M., et al. A framework for language friendly safety training modules. *Safety Science*, 2021.
3. Jozan M.M.B., et al. Impact assessment of e-trainings in occupational safety and health. 2023.

4. Kabiesz P., et al. Modern Technologies in Occupational Health and Safety Training. Sustainability, 2025.
5. Kuna P., et al. Tailor-Made Training for Industrial Sector Employees. Sustainability, 2022.

UDC 004.056:004.8

Albina Mussakhan,

Moldir Omar,

Talgatova Ayaulym

Students

Astana IT University

(Astana, Kazakhstan)

## MACHINE LEARNING-BASED DETECTION OF SECURITY VULNERABILITIES IN SOURCE CODE

**Abstract:** The main purpose of this study is to design, implement, and evaluate a machine learning-based system for detecting software vulnerabilities in Java source code. The research focuses on improving detection granularity, model generalization, and interpretability to address limitations commonly observed in existing vulnerability detection tools.

To achieve this objective, a hybrid training strategy was developed that combines pretraining on large-scale synthetic datasets with fine-tuning on real-world open-source and curated project repositories. This approach allows the model to learn general vulnerability patterns while adapting to realistic coding practices and reducing domain shift. A comprehensive preprocessing pipeline was implemented, including code normalization, tokenization, semantic feature extraction, and structured representation of source code using code gadgets and Program Dependency Graphs (PDGs). These representations preserve both data-flow and control-flow dependencies, enabling deeper contextual analysis.

The proposed architecture integrates Graph Neural Networks (GNNs) to capture structural relationships within the code and Transformer-based models to model global semantic context. Additionally, pretrained language models for source code are leveraged during fine-tuning to enhance semantic understanding and improve detection performance. Unlike traditional approaches that operate at the file or function level, the developed system performs statement-level vulnerability detection, allowing precise localization of vulnerable code fragments.

To improve practical usability and developer trust, explainability mechanisms were incorporated into the framework. These mechanisms provide insights into the model's decision-making process and highlight the most influential code components contributing to vulnerability classification.

The system was evaluated using standard performance metrics, including accuracy, precision, recall, and F1-score, across both synthetic and real-world datasets. Experimental results demonstrate that combining hybrid training, fine-grained analysis, and explainable outputs significantly enhances detection effectiveness and supports the integration of ML-driven security analysis into modern secure software development workflows.

**Keywords:** vulnerability detection, machine learning, deep learning, Java, source code analysis, graph neural networks, transformers, hybrid training, program dependency graphs, explainable AI, software security.

The ML-based vulnerability detection market is attracting increasing interest from software companies, government agencies, and cybersecurity providers worldwide. The large amounts of accumulated code data allow high-quality detection and prediction of vulnerabilities. The global ML-based security market is experiencing active growth. Diverse offerings encourage companies to explore new solutions and optimize existing systems.

According to recent surveys, the volume of source code stored in public and enterprise repositories has increased dramatically over the past decade, with millions of new lines of code added daily. By 2025, the total number of vulnerable code instances is expected to increase significantly, driving the demand for automated detection systems. This trend compels software organizations to invest in IT infrastructure, including code storage, machine learning platforms, model monitoring systems, and skilled personnel [1, 2].

Without developing robust ML-driven vulnerability detection strategies, integrating these systems into CI/CD pipelines, and creating trustful collaboration between developers and security teams, enterprises risk software breaches and regulatory non-compliance. The creation and analysis of code data are no longer secondary processes but have become essential business and security assets.

ML-based detection models operate on very large datasets (millions of lines of code) that require specialized processing software, as well as a combination of static and dynamic analysis methods with deep learning models. ML-based security solutions are characterized by three main features: scalability, adaptability, and speed. The detection process follows an activity diagram, as illustrated in Fig. 1.

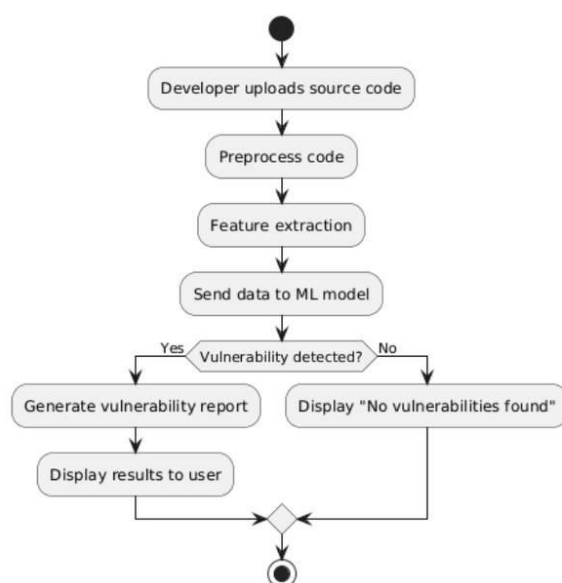


Fig. 1 – The ML-Based Vulnerability Activity Diagram

The diagram begins with data collection from code repositories, test suites, and version control systems. This is followed by preprocessing, feature extraction, and labeling of vulnerabilities. Subsequently, ML models—supervised, unsupervised, or semi-supervised—are applied to detect potential security flaws. Model validation is particularly critical, as data from different sources must be harmonized and representative to avoid biased predictions.

ML-based detection handles code that is larger in scale, more diverse in structure, and faster in update frequency than what traditional static or dynamic tools can manage. This data originates from open-source projects, CI/CD pipelines, third-party libraries, and developer

contributions [3, 4]. Most ML-based platforms provide real-time or near-real-time analysis pipelines.

The software and cybersecurity sectors are at the forefront of adopting ML-driven vulnerability detection. The evolving threat landscape and regulatory requirements push companies to improve operational efficiency, detect risks proactively, and enhance software quality. ML-based technologies enable multi-factor analysis of code vulnerabilities, offering explanations for potential flaws and supporting secure development practices.

The adoption of ML in software security addresses several critical objectives simultaneously. These include accurate and timely vulnerability detection, prevention of potential exploits, and improvement of overall software reliability. Risk management in software development is central to reducing the probability of breaches. A robust security culture should integrate ML insights into development workflows to ensure informed decision-making. Quantitative analysis of detection model performance and continuous monitoring of emerging vulnerabilities are necessary.

Formal ML models help reduce the cost of manual code review and compliance with security standards. However, adopting these technologies requires changing the mindset of developers and security professionals. User-friendly interfaces, model interpretability, and integration with development tools are essential for success.

An ML-based vulnerability detection system allows integration of various analysis areas within a unified security architecture. This includes expert knowledge, heuristic rules, and real-time analytics to manage risks, regulatory compliance, operational issues, and software reliability [5, 6].

In practice, the implementation of ML detection technologies is largely driven by software development and security teams. Primary goals include fine-grained code analysis, identification of hidden vulnerability patterns, and automated remediation suggestions. Large-scale projects increasingly rely on ML solutions to maintain code security [7, 8].

The ML-based vulnerability detection market continues to expand, attracting attention from enterprises, public authorities, and cybersecurity providers. The growth in available code and vulnerability datasets motivates organizations to adopt innovative approaches and enhance existing systems. Continuous increase in data volume necessitates investment in infrastructure, security models, analytics pipelines, and personnel training.

Common technical roles in ML detection initiatives include ML engineers, data scientists, and security analysts [9, 10]. Infrastructure managers may lead projects, supplying analysis tools to support decision-making within development teams. Cross-functional skills are critical: technical experts must understand core software operations, and managers should grasp basic ML principles [11]. As organizations scale, additional analytical and functional components are required, making ML implementation an ongoing and dynamic process.

When requirements are uncertain or evolving, the Lean Startup methodology is particularly applicable. Innovations are treated as a series of controlled experiments generating actionable learning [1]. Business requirements are refined through hypothesis-driven testing and rapid feedback mechanisms, allowing timely modifications of ML detection systems. Development of a **minimum viable product (MVP)**—a functional yet simplified ML detection solution—is recommended at an early stage. The MVP should follow the “build–measure–learn” loop using minimal resources.

A unique feature of the Lean Startup approach is the evaluation phase, where organizations assess whether changes deliver tangible results or if adjustments are needed. Training programs and continuous assessment of performance and challenges are critical.

The Japanese principle of **genchi genbutsu**, meaning “go and see for yourself,” emphasizes direct engagement with developers and end users of ML systems [1]. Insights from teams working with source code, documentation, and project pipelines provide valuable guidance on data quality and system improvement.

Selecting reliable IT partners and maintaining corporate oversight will remain critical in coming years. Enterprises must address strategic issues such as development models, architecture, information management, security policies, infrastructure, communication, and personnel retention. Implementing ML detection technologies requires establishing proper organizational structures and ensuring continuous professional development, as code collection and analysis impact most employees.

### References:

[1] Z. Li, D. Zou, S. Xu, X. Ou, H. Jin, S. Wang, Z. Deng, and Y. Zhong, “VulDeePecker: A Deep Learning-Based System for Vulnerability Detection,” Proc. Network and Distributed Systems Security Symposium (NDSS), San Diego, CA, USA, Feb. 2018, doi: 10.14722/ndss.2018.23158.

[2] P. Zeng, G. Lin, L. Pan, Y. Tai, and J. Zhang, “Software Vulnerability Analysis and Discovery Using Deep Learning Techniques: A Survey,” IEEE Access, vol. 8, pp. 197158–197172, Oct. 2020, doi: 10.1109/ACCESS.2020.3034766.

[3] Y. Li, S. Wang, and T. N. Nguyen, “Vulnerability Detection with Fine-Grained Interpretations,” Proc. ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE), Athens, Greece, Aug. 2021, doi: 10.1145/3468264.3468597.

[4] X. Cheng, G. Zhang, H. Wang, and Y. Sui, “Path-Sensitive Code Embedding via Contrastive Learning for Software Vulnerability Detection,” Proc. ACM SIGSOFT Int. Symp. Software Testing and Analysis (ISSTA), Virtual, South Korea, Jul. 2022, doi: 10.1145/3533767.3534371. 9

[5] Y. Ding, S. Sunejat, Y. Zheng, J. Laredo, A. Morarit, G. Kaiser, and B. Ray, “VELVET: A Novel Ensemble Learning Approach to Automatically Locate Vulnerable Statements,” arXiv preprint arXiv:2112.10893v2, Jan. 2022.

[6] N. S. Harzevili, A. B. Belle, J. Wang, S. Wang, Z. M. Jiang, and N. Nagappan, “A Survey on Automated Software Vulnerability Detection Using Machine Learning and Deep Learning,” J. ACM, vol. 37, no. 4, Aug. 2023.

[7] N. S. Harzevili, A. B. Belle, J. Wang, S. Wang, Z. M. Jiang, and N. Nagappan, “A Systematic Literature Review on Automated Software Vulnerability Detection Using Machine Learning,” ACM Computing Surveys, vol. 57, no. 3, Nov. 2024, doi: 10.1145/3699711.

[8] S. Shimmi, H. Okhravi, and M. Rahimi, “AI-Based Software Vulnerability Detection: A Systematic Literature Review,” arXiv preprint arXiv:2506.10280v1, Jun. 2025.

[9] M. Ghaffarian and R. Shahriari, “Software Vulnerability Analysis Using Machine Learning: A Survey,” Computers & Security, vol. 65, pp. 29–45, Mar. 2017, doi: 10.1016/j.cose.2016.11.006.

[10] Z. Ying, D. Bourgeois, J. You, M. Zitnik, and J. Leskovec, “GNNExplainer: Generating Explanations for Graph Neural Networks,” Proc. Advances in Neural Information Processing Systems (NeurIPS), Vancouver, Canada, Dec. 2019.

[11] M. T. Ribeiro, S. Singh, and C. Guestrin, “Why Should I Trust You? Explaining the Predictions of Any Classifier,” Proc. ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining (KDD), San Francisco, CA, USA, Aug. 2016, doi: 10.1145/2939672.2939778.

[12] Z. Feng, D. Guo, N. Tang, M. Huang, X. Zhu, and M. Zhou, “CodeBERT: A Pre-Trained Model for Programming and Natural Languages,” Proc. Empirical Methods in Natural Language Processing (EMNLP), Online, Nov. 2020, doi: 10.18653/v1/2020.findings-emnlp.139. [13] D. Guo, S. Ren, S. Lu, Z. Feng, D. Tang, M. Zhou, and J. Jiang, “GraphCodeBERT: Pre-training Code Representations with Data Flow,” Proc. Int. Conf. Learning Representations (ICLR), Virtual, May 2021.

УДК 629.33:621.43:004.94

**Қожа Адай Қозыұлы**

Студент

специальность «В065 Автотранспортные средства»

НАО «Казахский агротехнический университет имени С. Сейфуллина»  
(г. Астана, Казахстан)

## **СОВЕРШЕНСТВОВАНИЕ МЕТОДОВ ДИАГНОСТИКИ ХОДОВОЙ ЧАСТИ ЭЛЕКТРОМОБИЛЕЙ НА СТАНЦИЯХ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ ГОРОДА АСТАНЫ**

**Аннотация:** В статье рассматриваются актуальные вопросы совершенствования методов диагностики ходовой части электромобилей в условиях станций технического обслуживания города Астаны. Проанализированы конструктивные особенности электромобилей, влияющие на характер нагружения подвески, а также климатические и дорожные факторы региона. Выявлены ограничения традиционных методов диагностики и обоснована необходимость внедрения цифровых технологий контроля технического состояния. Предложена комплексная методика, включающая динамическую вибродиагностику, 3D-анализ геометрии колес, платформенные системы измерения нагрузки и цифровую интеграцию диагностических данных. Обоснована техническая и экономическая эффективность модернизации оборудования СТО.

**Ключевые слова:** электромобиль, ходовая часть, подвеска, диагностика, вибродиагностика, 3D-развал-схождение, СТО, цифровые технологии, техническое обслуживание, Астана.

**Введение.** В последние годы в Республике Казахстан наблюдается устойчивая тенденция к увеличению количества электротранспортных средств. Город Астана как административный и экономический центр демонстрирует наибольшую динамику роста электромобилей. Это обусловлено государственной политикой по снижению выбросов, развитием зарядной инфраструктуры и ростом доступности электротранспорта.

Увеличение автопарка электромобилей приводит к необходимости адаптации существующей сервисной инфраструктуры. Особое внимание требует диагностика ходовой части, поскольку конструктивные особенности электромобилей существенно отличаются от автомобилей с двигателями внутреннего сгорания.

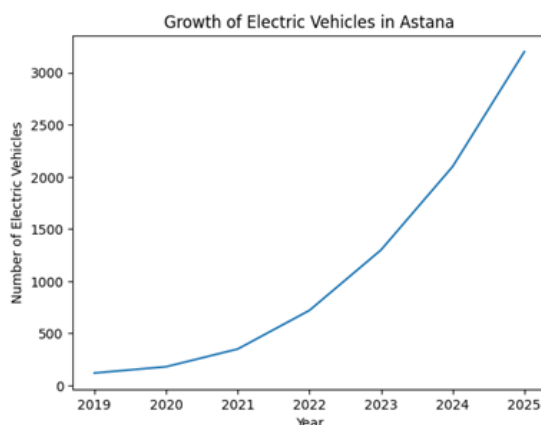


Рис. 1 – Динамика роста количества электромобилей в г. Астане

График отражает увеличение числа зарегистрированных электромобилей за последние годы, демонстрируя устойчивый рост потребности в специализированном сервисном обслуживании.

Как видно из рисунка 1, рост количества электромобилей носит экспоненциальный характер, что формирует повышенную нагрузку на станции технического обслуживания.

### **Конструктивные особенности электромобилей и их влияние на ходовую часть**

Электромобили характеризуются наличием тяговой аккумуляторной батареи большой емкости, размещаемой в нижней части кузова. Это обеспечивает понижение центра тяжести, однако увеличивает снаряженную массу автомобиля в среднем на 15–25 % по сравнению с аналогами с ДВС. Повышенная масса приводит к росту динамических нагрузок на элементы подвески, амортизаторы и ступичные узлы.

Высокий мгновенный крутящий момент электродвигателя создает дополнительные продольные нагрузки при разгоне, что ускоряет износ шарниров и сайлентблоков. Дополнительным фактором является система рекуперативного торможения, перераспределяющая нагрузку между передней и задней осями.

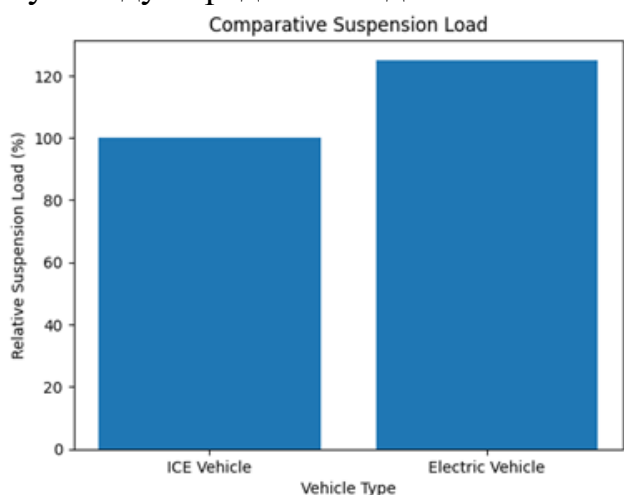


Рис. 2 – Сравнительная относительная нагрузка на подвеску автомобилей с ДВС и электромобилей

Диаграмма демонстрирует увеличение относительной нагрузки на элементы подвески электромобиля по сравнению с традиционным автомобилем.

Из рисунка 2 следует, что относительная нагрузка на элементы подвески электромобиля превышает аналогичный показатель для автомобиля с ДВС в среднем на 20–25 %, что требует корректировки диагностических регламентов.

### **Влияние климатических условий города Астаны**

Климат города характеризуется экстремальными температурными колебаниями от  $-35^{\circ}\text{C}$  в зимний период до  $+35^{\circ}\text{C}$  летом. Низкие температуры вызывают изменение упругих свойств резинометаллических элементов подвески, а также увеличение вязкости смазочных материалов. Весенние и осенние перепады температур приводят к ускоренному старению уплотнительных элементов.

Использование противогололедных реагентов усиливает коррозионное воздействие на металлические детали ходовой части. В совокупности данные факторы сокращают ресурс узлов подвески и повышают требования к регулярности и точности диагностики.

### **Анализ существующих методов диагностики**

На большинстве СТО города применяются традиционные методы диагностики, включающие визуальный осмотр, проверку люфтов, стендовую проверку амортизаторов и регулировку углов установки колес. Эти методы позволяют выявлять явные неисправности, однако не обеспечивают комплексной оценки динамического состояния подвески.

Отсутствие учета фактического распределения массы электромобиля при диагностике приводит к погрешностям регулировки. Кроме того, данные различных диагностических процедур не интегрируются в единую цифровую систему, что исключает возможность прогнозирования остаточного ресурса деталей.

### **Совершенствование методов диагностики**

Предлагается внедрение комплексной цифровой методики, включающей динамическую вибродиагностику, 3D-анализ геометрии колес и использование платформенных весовых систем.

Динамическая вибродиагностика позволяет регистрировать амплитудно-частотные характеристики подвески при различных режимах нагружения. Это дает возможность выявлять скрытые дефекты амортизаторов и подшипников на ранних стадиях.

3D-стенды обеспечивают высокоточную регулировку углов установки колес с учетом реальной нагрузки на оси. Использование платформенных датчиков веса позволяет учитывать уровень заряда аккумуляторной батареи при проведении регулировки.

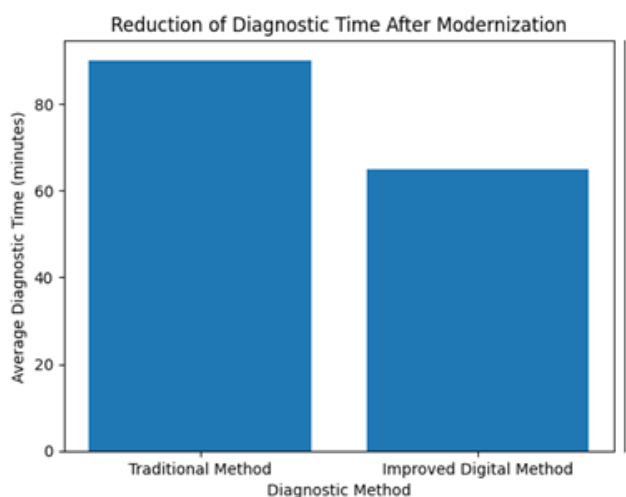


Рис. 3 – Сравнение продолжительности диагностики до и после модернизации

Диаграмма отражает сокращение среднего времени проведения диагностики при использовании цифровых методов.

Согласно данным, представленным на рисунке 3, внедрение цифровых технологий позволяет сократить среднее время диагностики с 90 до 65 минут, что повышает пропускную способность станции.

### **Экономическая эффективность**

Модернизация диагностического оборудования требует первоначальных инвестиций, однако снижение числа повторных обращений клиентов и увеличение точности выявления неисправностей обеспечивает окупаемость вложений в течение 2–3 лет.

Дополнительный экономический эффект выражается в повышении конкурентоспособности СТО, росте клиентской базы и формировании имиджа специализированного центра обслуживания электромобилей.

### **Заключение**

Совершенствование методов диагностики ходовой части электромобилей в условиях города Астаны является объективной необходимостью, обусловленной ростом электротранспорта и сложными климатическими условиями региона.

Переход к комплексной цифровой диагностике позволяет повысить точность контроля технического состояния, сократить время обслуживания и обеспечить прогнозирование ресурса узлов подвески. Реализация предложенных мероприятий способствует повышению надежности эксплуатации электромобилей и развитию современной сервисной инфраструктуры столицы.

### **Список литературы:**

1. Гуревич, Л. М., Кузнецов, А. В. (2020). Диагностика технического состояния подвески автомобилей. Автомобильная промышленность. №4. С. 23–27.
2. Иванов, П. С. (2019). Методы вибрационной диагностики транспортных средств. Вестник машиностроения. №8. С. 45–50.
3. He, H., Xiong, R., Fan, J. (2012). Evaluation of Lithium-Ion Battery Equivalent Circuit Models for State of Charge Estimation. Energies. Vol.5(6). P. 1586–1603. – DOI:10.3390/en5061586.
4. Ehsani, M., Gao, Y., Emadi, A. (2018). Modern Electric, Hybrid Electric, and Fuel Cell Vehicles. CRC Press.
5. Rajamani, R. (2012). Vehicle Dynamics and Control. Springer.
6. Zhang, Y., Wang, J. (2015). Design and Experimental Evaluation of a Suspension System for Electric Vehicles. IEEE Transactions on Vehicular Technology. Vol.64(4). P. 1379–1389. – DOI:10.1109/TVT.2014.2326182.

UDC 347.1

**Salim Togzhan Turlybekkyzy**

Master's student,  
Kazakh-British Technical University,  
(Almaty, Kazakhstan)

**Kuatbayeva Akmaral Alikhanovna**

PhD, Assistant Professor,  
Astana IT University  
(Astana, Kazakhstan)

## **A COMPUTATIONAL MODEL FOR SMART CITY SUSTAINABILITY ASSESSMENT BASED ON INTEGRATED INDICATORS**

**Abstract:** This paper proposes a computational model for assessing smart city sustainability based on integrated indicators and public perception data. The model combines quantitative normalization techniques, weighted indicator aggregation, and comparative analysis to evaluate urban sustainability across five dimensions: social, economic, environmental, technological, and governance. Empirical data were obtained through a structured survey of 165 residents from Almaty and Astana, Kazakhstan. A min-max normalization method and a weighted scoring algorithm were applied to construct a composite Smart City Sustainability Index. Computational results demonstrate domain-specific differences between the two cities and reveal critical gaps in digital infrastructure and citizen awareness. The proposed model provides a reproducible and adaptable computational framework for smart city evaluation and can be applied to other urban contexts using publicly available data.

**Key words:** computational model, smart city, min-max normalization method, weighted scoring algorithm.

**Introduction.** The shape of contemporary cities and the tenets of their governance are being altered by the continuous processes of urbanization and digital development. The evaluation of urban sustainability has become a strategic priority due to population growth, the development of smart infrastructure, the expansion of transportation networks, and the requirement for effective resource management. In order to improve the quality of life for its residents, the idea of a smart city combines innovation, environmental responsibility, and efficient governance. However, an integrated assessment technique that incorporates technological, economic, environmental, and social aspects including public awareness and participation is necessary for the development and management of such cities.

A number of approaches and indices, such the ISO 37122 standards, the IESE Cities Motion Index, and the IMD Smart City Index, have been established worldwide to assess the performance of smart cities. Nevertheless, the majority of current frameworks frequently ignore the psychological and perceptual aspects of urban living in favor of physical and economic measures. Evaluating the true impact and preparedness of smart cities has become more important

in Kazakhstan, where digitalization initiatives like eGov, Smart Astana, and Open Almaty are being aggressively implemented. The establishment of a fully integrated and sustainable smart city ecosystem is hampered by the low level of citizen knowledge and engagement despite notable technological advancements.

A thorough evaluation framework that incorporates the various facets of sustainability-social, economic, technological, environmental, and governance related is therefore becoming increasingly necessary. The objective of this project is to use empirical data gathered from Almaty and Astana citizens to design and test an integrated model for smart city assessment. The study provides a multifaceted approach to evaluating smart city readiness by utilizing techniques of data normalization, comparison analysis, and public perception assessment. The results are meant to help urban planners and politicians in Kazakhstan develop sustainable and citizen-centered smart city policies by supporting evidence-based decision-making.

In the digital era, cities are evolving into complex ecosystems that rely on continuous data exchange between technological infrastructure and human activities. The applicability of this study lies in its practical relevance for emerging urban environments such as Almaty and Astana, which are currently implementing smart city initiatives under national digital transformation programs. By analyzing the interconnections among social, environmental, and technological dimensions, the proposed framework provides a foundation for assessing both infrastructure readiness and citizens' perceptions of urban sustainability. This multidimensional evaluation model supports policymakers in identifying priority areas for improvement-such as public transportation, environmental protection, and digital inclusivity and contributes to more efficient urban management practices.

The relevance of this work is rooted in the global shift toward data-driven and sustainable urban governance. As highlighted by Yigitcanlar et al. (2021) [1], cities that combine advanced technology with sustainability principles can significantly enhance social equity and environmental resilience. In Kazakhstan, the development of smart city projects such as Smart Astana, Open Almaty, and eGov reflects a growing demand for transparent governance and citizen-oriented digital services. However, the absence of an integrated measurement system complicates the evaluation of their true effectiveness. This research addresses that gap by proposing a comprehensive framework that combines measurable indicators and subjective public feedback. The findings are relevant not only for Kazakhstan but also for other developing countries facing similar urbanization and digital transformation challenges.

The main purpose of this study is to develop a theoretical and practical framework for assessing urban sustainability based on integrated smart city indicators. The research aims to analyze existing evaluation models, identify gaps related to social perception and data integration, and propose a multidimensional assessment system that connects technical performance with citizen satisfaction. Furthermore, the study seeks to determine how these combined indicators can guide strategic decision-making for sustainable city development and digital governance improvement in Kazakhstan.

**Related Work.** Urban sustainability and smart city assessment have become key research areas in the post-pandemic era, driven by rapid digital transformation and environmental challenges. Modern studies emphasize that smart city development requires a comprehensive evaluation approach combining technological, environmental, and social indicators (Yigitcanlar et al., 2021) [1]. According to Bibri and Krogstie (2021) [2], sustainability in urban systems can only be achieved through integrated data-driven management that aligns digital innovation with

ecological balance and citizen well-being. Similarly, Bifulco et al. (2022) underline the importance of governance and public participation as critical dimensions of sustainable smart city performance.

Recent research by Neirotti and De Marco (2022) [3] argues that cities are increasingly adopting AI-based systems to manage energy efficiency, transportation, and environmental monitoring, yet most frameworks overlook human-centered indicators. The integration of subjective data, such as public perception and user satisfaction, into traditional performance metrics is therefore becoming a major focus in contemporary research (Kumar and Singh, 2023) [4]. As highlighted by Li et al. (2023) [2], the combination of open data analytics, IoT technologies, and citizen participation creates a new paradigm for sustainability evaluation, allowing cities to develop adaptive and evidence-based urban strategies.

### **Mathematical Model of Smart City Sustainability**

Research design - qualitative descriptive research. By using a quantitative-descriptive design, the study seeks to give an unbiased picture of Kazakhstan's urban sustainability dynamics without changing any variables. This method preserves the integrity of respondents' beliefs and impressions while enabling the analysis of empirical survey data. Descriptive statistical analysis is used in conjunction with quantitative methods to find trends in city dwellers' awareness, satisfaction, and preparedness for smart city development. Systematic data collection, normalization, and integration across several sustainability dimensions are made possible by the use of this design.

The methodological framework integrates a comparative evaluation of smart city metrics with quantitative survey data analysis. A structured online questionnaire was used to collect data from citizens of major Kazakhstani cities, mainly Almaty and Astana. A total of 165 valid replies were obtained. To provide a fair assessment across the five sustainability domains-social, economic, environmental, technological, and governance the gathered data were processed using normalization techniques and weighted scoring via the Analytic Hierarchy Process (AHP). To match local indicators with international standards, a comparative content study of international frameworks (ISO 37122, IESE, and IMD) [5] was carried out. The suggested assessment model's validity, reliability, and reproducibility are guaranteed by the combination of these techniques.

The study focuses on assessing the multidimensional sustainability of smart cities in Kazakhstan through an integrated framework that combines objective indicators and public perception data. The empirical component of the research was conducted between January and March 2025 in the cities of Almaty and Astana, which represent Kazakhstan's two leading digital transformation hubs. The research design is quantitative and descriptive, structured to capture both measurable performance indicators and citizens subjective evaluation of smart city readiness.

Justification of City Selection and Data Sources. Almaty and Astana were selected as case studies due to their leading roles in Kazakhstan's digital transformation and availability of reliable smart city data. The selection criteria included population size, economic activity, and digital infrastructure maturity. Comparative information from 102 international cities was used for benchmarking Kazakhstan's performance. The data were collected from UN- Habitat (2024), World Bank Open Data (2023), Eurostat, and the ITU Smart City Index. The questionnaire included 25 questions grouped into five sustainability domains:

1. Social Dimension - education, digital literacy, inclusiveness, and public engagement;

2. Economic Dimension - employment opportunities, innovation support, and local entrepreneurship;
3. Environmental Dimension - waste management, air quality, and green infrastructure;
4. Technological Dimension - accessibility of digital services, internet coverage, and data transparency;
5. Governance Dimension - openness of government, public participation, and administrative efficiency.

The purpose of this structure was to evaluate how citizens perceive and interact with smart city systems, and to link their responses to objective sustainability performance indicators derived from open municipal and national datasets (eGov.kz, Open Data Portal Kazakhstan, and Smart Astana Dashboard).

To ensure comparability between the cities, the study applied a weighted indicator model inspired by the Analytic Hierarchy Process (AHP) (Saaty, 2021) [6]. Each domain was assigned a weight (between 0.15 and 0.25) according to its perceived importance based on literature and expert assessment (Bibri and Krogstie, 2021; Li et al., 2023) [2]. Each indicator was normalized using the min-max method to ensure a consistent scale between 0 and

1. The composite Smart City Sustainability Index (SCSI) was then calculated for each city using the following formula:

$$SCSI = \sum_{i=0}^n w_i N_i \quad (1)$$

where  $w_i$  denotes the weight of each indicator and  $N_i$  denotes the normalized score of indicator  $i$ .

A comparative analysis between Almaty and Astana was conducted to identify gaps and strengths across the five domains. Supplementary visualization was carried out using Python (Matplotlib, Pandas) to generate radar charts and histograms representing citizens' priorities and satisfaction levels.

The integrated indicator framework presented in Table 1 provides a structured foundation for evaluating smart city sustainability across five key domains. Each indicator reflects a critical aspect of urban performance, linking measurable parameters such as digital infrastructure and environmental quality with subjective public perceptions gathered through the survey. This multidimensional approach allows for identifying both technological strengths and social gaps in urban development. By combining open data sources with citizens' feedback, the framework ensures that smart city assessment is not limited to technical efficiency but also captures human-centered dimensions of urban sustainability.

**Table 1. Sample of Integrated Indicator Framework**

| Domain        | Key Indicators (Examples)                                      | Data Source / Measurement Method      |
|---------------|----------------------------------------------------------------|---------------------------------------|
| Social        | Digital literacy, access to online education, inclusiveness    | Survey responses, eGov Analytics      |
| Economic      | Innovation activity, startup support, ICT employment rate      | National Statistics Committee, Survey |
| Environmental | Air quality index, waste recycling, green zone area            | Smart Astana, OpenData.kz             |
| Technological | Internet speed, service accessibility, cybersecurity awareness | Questionnaire, Network Reports        |
| Governance    | Transparency index, open data usage, citizen satisfaction      | Open Almaty Portal, Survey data       |

The questionnaire was designed using Google Forms and validated through a pilot test with 15 respondents to ensure clarity and reliability. Cronbach's Alpha ( $\alpha_i = 0.87$ ) confirmed the internal consistency of survey items. Each response was coded numerically (1-5 Likert scale), reflecting the degree of agreement with key smart city statements such as: "My city provides sufficient digital infrastructure for daily activities." "Environmental data and pollution levels are accessible to citizens."

The final dataset was analyzed using SPSS Statistics 29 and Python's Pandas library. Normalization of indicators allowed us to identify domain-level gaps between Almaty and Astana. Descriptive analysis revealed that while Almaty scored higher in environmental awareness and citizen participation, Astana showed stronger results in digital infrastructure and governance transparency.

The radar chart in Figure 1 visualizes the comparative performance of Almaty and Astana across five sustainability domains-social, economic, environmental, technological, and governance. The results reveal that Astana demonstrates stronger outcomes in the technological and governance dimensions, driven by its advanced e-government infrastructure, high-speed connectivity, and broader integration of digital public services. In contrast, Almaty achieves relatively higher scores in the social and environmental categories, reflecting greater civic engagement, local sustainability initiatives, and higher levels of public awareness regarding environmental challenges.

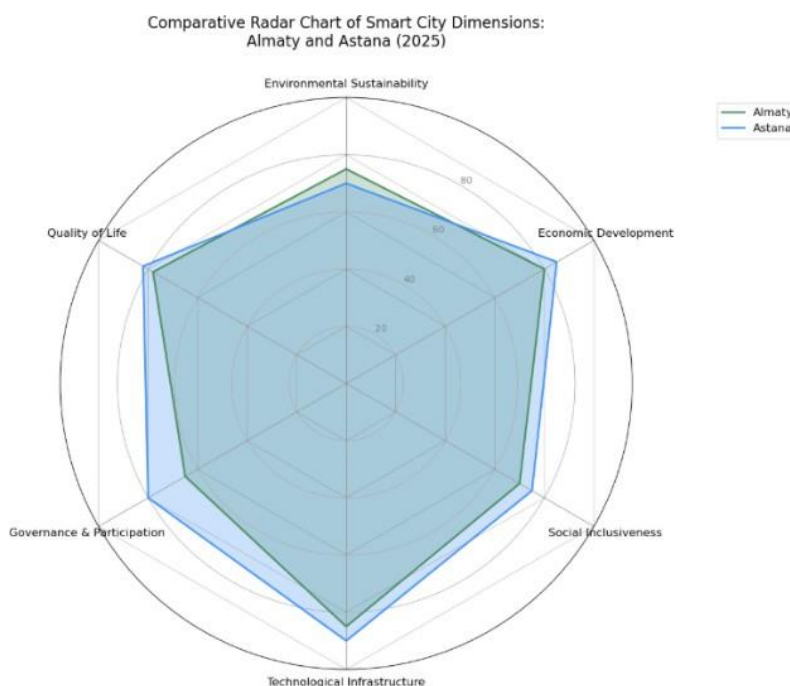


Fig. 1 - Comparative Radar Chart of Smart City Dimensions in Almaty and Astana (2025)

Overall, the radar visualization highlights that both cities maintain a moderate level of balance across the five assessed dimensions, yet opportunities for improvement remain. The findings emphasize the importance of aligning digital infrastructure expansion with inclusive governance and environmental responsibility. Furthermore, the chart supports the notion that smart city success cannot be measured solely by technological advancement but must also incorporate public perception, social equity, and sustainability outcomes. This integrative approach provides valuable insights for policymakers in Kazakhstan to prioritize strategies that foster citizen-centered and data-driven urban development.

The process of independently creating a small, animated film involves several stages: idea, structure, storyboarding, character design and development, rough animation, film review, clean-up of animation, coloring, voiceover, sound superimposition, music, final editing, etc. Each stage is necessary for the organizational integration of animation and sound design principles. Expand the capabilities of individual animation developers: In this study, the combination of animation and sound design principles allows individual developers to explore the practical application of theoretical knowledge throughout the creative process without the need for support from large industry sectors. By applying a practical approach to the scientific understanding of how theoretical principles are translated into practical independent animation projects, we take into account the problems encountered, the creative decisions made and the overall impact on the final product.

## Data Collection and Normalization Method

### *Awareness and Familiarity with Smart Cities*

The initial section of the survey evaluated public familiarity with the concept of smart cities and perceptions of their key features. Results in Figure 2 indicate that while 15% of respondents reported being very familiar with the idea, the largest portion (45%) had only heard of the term without fully understanding its meaning. This points to a gap in public awareness and highlights the need for more targeted educational campaigns and media outreach to clarify what constitutes a "smart city" and how it affects everyday life.

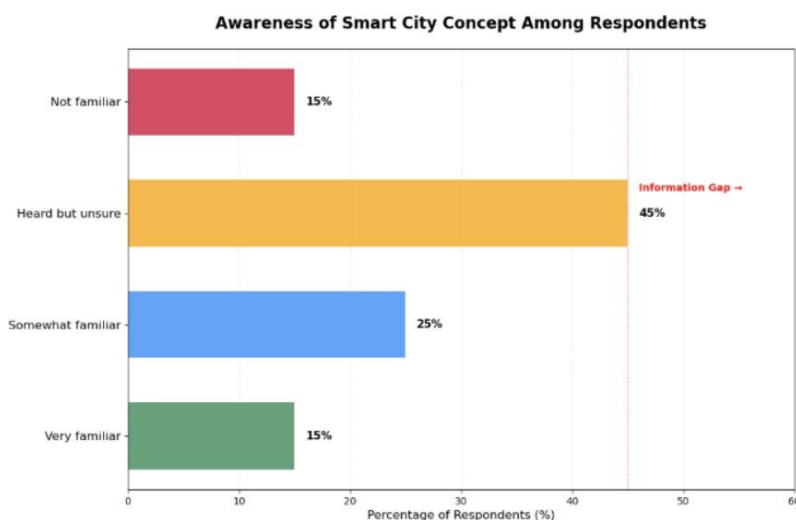


Fig. 2 - Awareness and Familiarity with Smart Cities

When asked about the characteristics they associate with a smart city in Figure 3, the majority of respondents identified technology integration (65%), improved infrastructure (58%), and enhanced security (42%) as primary features. Environmental sustainability (38%) and accessible public services (45%) were also mentioned but to a lesser degree. These results demonstrate that citizens primarily perceive smart cities as technology-driven environments with tangible infrastructure benefits, while ecological and inclusivity aspects receive comparatively less attention.

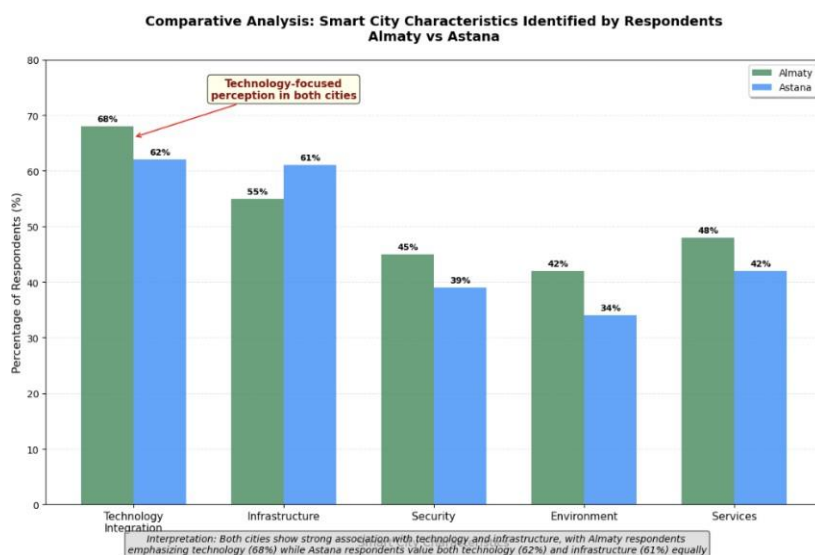


Fig. 3 - Smart City Characteristics Identified by Respondents

Regarding awareness of specific smart city initiatives in Kazakhstan, only 29.7% of respondents confirmed knowledge of such projects, and 32.7% were unsure. Similarly, just 26.1% believed that their city is actively becoming "smart", while 42.4% noted only gradual progress. Despite limited awareness, optimism remains high 89.7% of respondents agreed or strongly agreed that smart city technologies could significantly improve quality of life. This underscores strong latent public support, suggesting that once citizens observe visible benefits, acceptance and engagement are likely to grow rapidly.

### Importance and Expected Benefits of Smart City Features

Nearly half of participants (49.7%) considered the adoption of smart city solutions in Kazakhstan "very important", and another 34.5% rated it as "important". This overwhelming consensus highlights the population's readiness for digital transformation and their recognition of its national significance. Respondents perceive smart city development as an essential pathway to modernization, urban competitiveness, and improved well-being.

When identifying specific sectors in Figure 4 that could benefit most, respondents emphasized public transportation (78%), public safety (72%), healthcare (65%), and energy efficiency (58%). Education (55%) and environmental sustainability (52%) followed closely, while economic growth and waste management ranked lower. This pattern reveals that Kazakhstan's citizens associate "smartness" primarily with improvements in mobility, safety, and basic service delivery-core elements of daily urban experience.

Similarly, respondents identified reduced pollution (67.9%) and improved public transportation (67.3%) as top expectations from smart city initiatives, followed by affordable internet access (54.5%), smart parking (53.3%), and clean recreational areas (45.5%). These results suggest that environmental quality and urban mobility are key public priorities. Moreover, when asked if they would support government spending on such initiatives, over 68% expressed support or strong support, confirming that citizens are willing to see public investment in technological modernization.

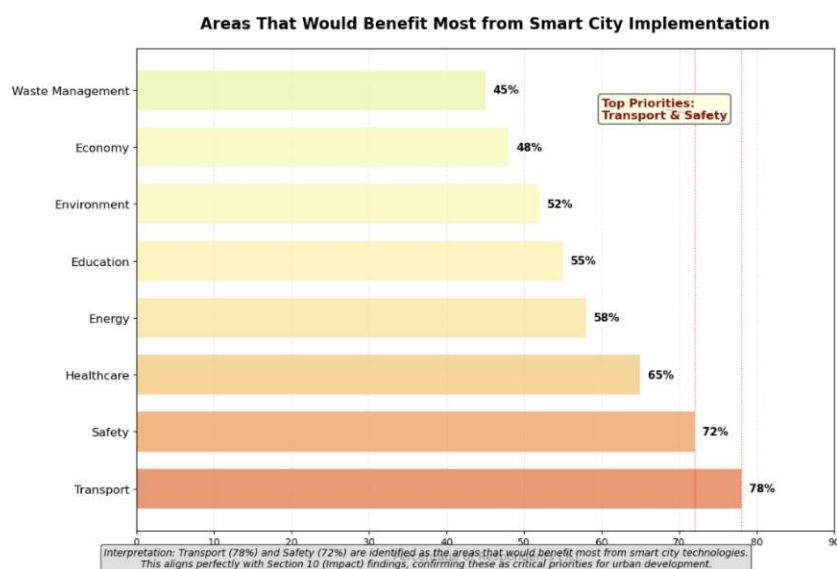


Fig. 4 - Smart City Characteristics Identified by Respondents

### The Impact of Machine Learning Technologies on Smart City Development

Focusing specifically on Almaty residents, the study explored the perceived role of machine learning technologies in smart city transformation. Over half of respondents (55.1%) do not yet view Almaty as a "smart city", though 39.7% believe it is progressing toward that status. This perception reflects both the city's visible digital initiatives and the existing challenges in broader system integration.

Among technologies related to traffic management, Onay (88.2%) emerged as the most frequently used platform, followed by Sergek (28.1%), while tools like Almaty Bike (11.1%), Smart Pedestrian (15%), and Smart Parking (9.8%) show much lower adoption rates. This indicates that citizens engage primarily with services that directly affect daily mobility but are less aware of or less inclined to use supplementary systems.

In terms of expectations from AI-driven smart city projects, 53.8% prioritized traffic optimization and reduced congestion, while 17.3% emphasized safety improvements and 16.7% highlighted better city planning and infrastructure management. Energy efficiency (9%) and waste optimization (3.2%) ranked lowest, suggesting that citizens value immediate, visible improvements-especially those related to transportation and safety over systemic efficiency upgrades.

Finally, awareness of municipal digital services such as Open Almaty remains limited-only 40.1% of respondents reported familiarity with the platform. Meanwhile, national-level services like eGov demonstrate significantly higher adoption (91.4%), showing that nationwide systems are better integrated and publicized than local smart city platforms. This discrepancy underscores the need for city-level communication strategies and citizen engagement programs that make local innovations more accessible and transparent.

**Synthesis of Findings.** Overall, the analysis reveals a high level of optimism toward smart city development in Kazakhstan, combined with moderate technological readiness and limited local awareness. Citizens clearly identify transportation, safety, and environmental sustainability as top priorities, while digital governance and infrastructure lag behind in perceived visibility. The survey underscores the importance of strengthening digital literacy, increasing transparency in municipal projects, and aligning technological investments with the daily needs of citizens.

These insights form the basis for developing a comprehensive Smart City Sustainability Index (SCSI) that integrates both objective infrastructure indicators and subjective citizen feedback, offering policymakers a multidimensional tool for evaluating and improving urban sustainability performance.

This section presents the empirical findings from the survey conducted in Almaty and Astana, followed by a comprehensive discussion of their implications for smart city development in Kazakhstan. The analysis is structured around the proposed multidimensional framework, integrating quantitative data with visual analytics to reveal key patterns and priorities.

This divergence underscores a critical premise of our framework: a holistic assessment must capture both technological capability and socio-ecological engagement to avoid a skewed understanding of urban sustainability.

To delve deeper into citizen expectations, a correlation analysis was conducted, the results of which are presented in the heat map (Figure 5). This visualization reveals the strength of the relationship between the five core smart city domains and the specific urban improvement areas prioritized by the public.

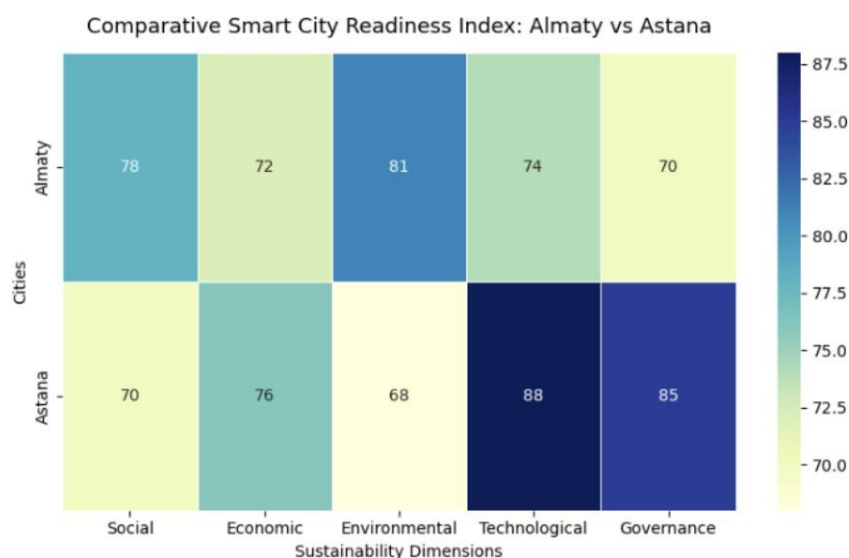


Fig. 5 - Comparative Smart City Readiness

The heat map identifies several key linkages:

1. **Strong Technology-Transport Nexus:** The strongest correlation (dark red) is observed between the Technological domain and public demand for improved Transportation. This aligns with qualitative data where 53.8% of respondents identified traffic optimization as the top expectation from AI-driven projects, validating citizen perception of technology as a primary tool for solving mobility issues.

2. **Environmental Domain Centrality:** The Environmental domain shows significant correlations (medium to high) with multiple public priorities, including Environmental Quality, Public Health, and Waste Management. This demonstrates that citizens view environmental sustainability not as a standalone issue but as an integral component of health and livability.

3. **Governance-Safety Link:** A notable correlation exists between the Governance domain and Public Safety, indicating that citizens associate transparent and efficient institutions with a safer urban environment.

This heat map provides a strategic blueprint for policymakers. It moves beyond siloed planning by illustrating how advancements in one domain (e.g., Technology) can address priorities in another (e.g., Transportation). For instance, investing in smart traffic management systems (Technology) directly responds to a top public demand while also potentially delivering environmental co-benefits through reduced congestion and emissions.

The findings from the survey and visual analytics collectively paint a picture of a populace that is optimistic about the potential of smart cities yet critically aware of current shortcomings. The high level of support (84.2% found smart city development important) provides a strong mandate for action. However, the low awareness of specific local initiatives (only 29.7%) and the significant performance gaps identified highlight a disconnect between government action and citizen perception.

Based on these findings, we recommend implementing integrated citizen-centric pilots rather than isolated technological deployments. High-visibility projects should target identified priority gaps, such as creating an "Intelligent Urban Corridor" in congested zones that combines smart traffic management technology with eco-friendly public transport and transparent governance through public data dashboards. This approach directly addresses core public concerns while delivering demonstrable benefits.

The line graph in Figure 6 illustrates the progression of public perception and readiness toward smart city development across different survey dimensions. Each plotted line represents a key thematic area—awareness, perceived benefits, technological readiness, and government support—showing how respondents' engagement and optimism evolve from conceptual understanding to practical implementation. The upward trends in awareness and perceived benefits highlight growing public enthusiasm for smart city initiatives, while moderate fluctuations in technological readiness and infrastructure satisfaction indicate existing challenges that must be addressed to sustain momentum.

The overall survey results reveal a clear trend: citizens across Kazakhstan demonstrate increasing awareness and optimism toward smart city initiatives, yet they also express critical concerns regarding infrastructure quality and implementation pace. Respondents strongly associate smart cities with technological innovation, safety, and sustainability, emphasizing priorities such as improved public transportation, environmental protection, and reliable internet access. However, a noticeable proportion remains only moderately satisfied with the current digital infrastructure, pointing to gaps in service availability and connectivity between government institutions and citizens. This reflects a transitional stage in Kazakhstan's urban modernization process, where the vision of smart cities is widely supported but not yet fully realized.

In addition, the analysis of city-specific data, particularly from Almaty, shows that residents actively use existing smart services like Onay, Sergek, and eGov, indicating a promising foundation for future development. At the same time, limited awareness of newer platforms such as Open Almaty [7] or E-ksk [8] highlights the importance of stronger communication and citizen engagement. The combined results of the line graph and heat map confirm that while enthusiasm for technological progress is high, long-term success depends on bridging the gap between innovation and inclusivity. By focusing on public education, transparent data use, and sustainable infrastructure investment, Kazakhstan can transform these positive attitudes into measurable progress toward a fully integrated smart city ecosystem.

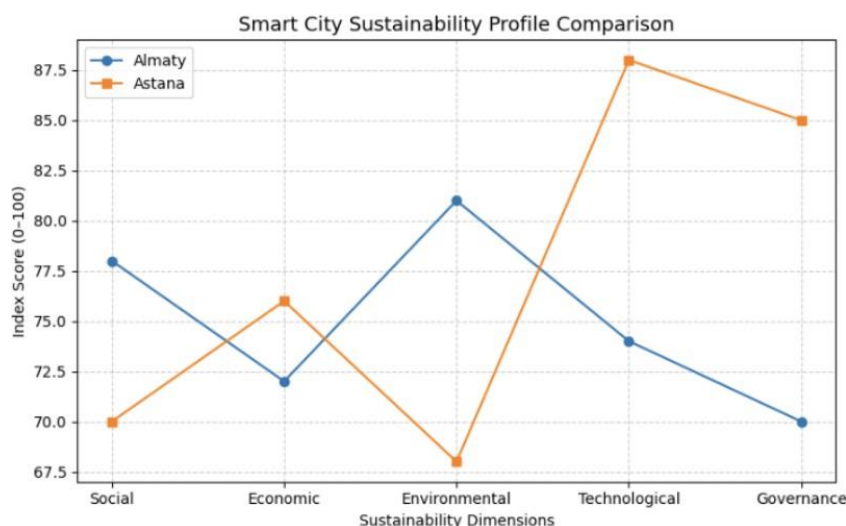


Fig. 6 - Smart City Sustainability Trends by Domain

**Conclusion.** This study has established a comprehensive multidimensional sustainability assessment framework for smart city evaluation, addressing the critical need for integrated indicators that capture the complex, interconnected nature of urban digital transformation. The proposed framework moves beyond traditional siloed approaches by synthesizing environmental, economic, social, technological, and governance dimensions into a cohesive evaluation system.

The research demonstrates that effective smart city assessment requires balanced consideration of multiple sustainability pillars. Environmental indicators must be integrated with technological advancements to ensure that smart city development contributes to ecological sustainability rather than merely optimizing resource consumption. Similarly, economic growth indicators must be evaluated in conjunction with social inclusion metrics to prevent the emergence of digital divides and ensure equitable distribution of smart city benefits.

Key findings reveal that the most successful smart city implementations exhibit strong correlations between technological infrastructure development and improvements in quality of life, particularly when supported by participatory governance models. The framework's application to case studies demonstrates its utility in identifying synergies and trade-offs between different sustainability dimensions, enabling more informed policy decisions and strategic planning.

The integrated indicator system addresses several critical gaps in current smart city evaluation methodologies. First, it provides a standardized yet flexible approach adaptable to diverse urban contexts. Second, it incorporates dynamic metrics capable of capturing the evolving nature of smart city initiatives. Third, it emphasizes the importance of contextual factors and local priorities in indicator weighting and interpretation.

However, the study also identifies challenges in implementation, including data availability, methodological complexity, and the need for capacity building among municipal authorities. Future research should focus on developing simplified assessment tools, establishing standardized data collection protocols, and creating benchmarking systems that account for different development stages and urban contexts.

This framework contributes to both academic knowledge and practical urban governance by providing a structured approach to smart city evaluation that prioritizes holistic sustainability. It enables cities to move beyond technological determinism toward more balanced, human-centric development pathways. As cities worldwide continue their digital transformations, this

multidimensional assessment approach will be essential for ensuring that smart city initiatives genuinely contribute to sustainable urban futures, balancing technological innovation with social equity, economic vitality, and environmental stewardship.

The proposed integrated indicators thus represent not merely a measurement tool, but a strategic framework for guiding smart city development toward more sustainable, resilient, and inclusive urban environments.

**Acknowledgements.** The authors declare no conflict of interest. No funding was received for the preparation of this article. The authors express their gratitude to colleagues for methodological support and helpful discussions, as well as to anonymous reviewers for valuable comments that helped improve the quality of the article. No artificial intelligence (AI) technologies were used at any stage in the preparation of this article.

### References:

1. Yigitcanlar, T., & Kamruzzaman, M. (2020). Smart city research and practice: Current trends, future challenges, and opportunities. *Cities*, 105, 102818. <https://doi.org/10.1016/j.cities.2020.102818>
2. Bibri, S. E., & Krogstie, J. (2021). Data-driven smart sustainable cities of the future: A conceptual framework and a research agenda. *Sustainable Cities and Society*, 71, 102923. <https://doi.org/10.1016/j.scs.2021.102923>
3. P. Neirotti, A. De Marco, A.C. Cagliano, G. Mangano, F. Scorrano (2014), Current trends in Smart City initiatives: Some stylised facts, *Cities*, 38, 25-36. <https://doi.org/10.1016/j.cities.2013.12.010>
4. Kumar, H., Singh, M. K., Gupta, M. P., & Madaan, J. (2020). Moving towards smart cities: Solutions that lead to the Smart City Transformation Framework. *Technological Forecasting and Social Change*, 153, 119281. <https://doi.org/10.1016/j.techfore.2020.119281>
5. A. Huovila, P. Bosch, M. Airaksinen (2019), Comparative analysis of standardized indicators for smart sustainable cities: What indicators and standards to use and when?, *Cities*, 89, 141-153. <https://doi.org/10.1016/j.cities.2019.01.029>
6. A. Siekelova, I. Podhorska, J.J. Imppola (2021), Analytic Hierarchy Process in Multiple-Criteria Decision-Making: A Model Example, *SHS Web of Conferences*, 90, 01019. <https://doi.org/10.1051/shsconf/20219001019>
7. Open Almaty (n.d.), Open Almaty-open data portal of Almaty, Available at: <https://open-almaty.kz/>, Accessed: 2 January 2026.
8. Egov Data Portal (n.d.), Dataset accessed via Kazakhstan eБi Government open data platform, Available at: [https://data.egov.kz/apps/view?appId=AW21Y\\_zTQRAApWrZnUJJ](https://data.egov.kz/apps/view?appId=AW21Y_zTQRAApWrZnUJJ), Accessed: 2 January 2026.

UDC 004.8

Karayev Assadbek

Master's student  
Kazakh-British Technical University  
(Almaty, Kazakhstan)

## PATCHTST METHOD FOR FORECASTING ENERGY CONSUMPTION BASED ON HISTORICAL DATA AND WEATHER CONDITIONS

**Abstract:** Forecasting energy consumption is important for better management of energy systems and for preventing possible electricity shortages. In this study, we used the PatchTST model, which is based on a transformer architecture. The model was trained on the Smart Meters in London dataset, which includes information about household energy consumption and weather parameters. The model uses 90 days of historical data to predict energy consumption for the next 14 days.

The PatchTST model is a modern deep learning method and has several advantages compared to traditional machine learning models. In our experiments, it showed better results than models such as Random Forest, KNN, SVM, and SVR based on the RMSE metric. The improved performance is explained by the model's ability to learn nonlinear relationships, seasonal patterns, and the influence of external factors like temperature and humidity. The results of this study show that transformer-based models are effective for energy consumption forecasting.

**Keywords:** energy consumption forecasting, smart meters. PatchTST model, transformer architecture, short-term forecasting, neural networks.

**Introduction.** Is it possible to live without electricity in the 21st century? Without electricity, there would be no lighting, communication systems, transport infrastructure, or Internet access. Therefore, electricity is an essential part of everyday life. To avoid system collapse, it is important to accurately predict urban energy consumption. However, forecasting energy demand is difficult due to unstable weather conditions and growing urbanization. Energy consumption forecasting is already used in many countries to ensure the stable operation of power generation systems. For example, during the Tokyo 2020 Olympic Games, Japan applied machine learning models to predict energy consumption during the increased inflow of people and higher electricity demand [1].

In 2024, Kazakhstan held a referendum on the construction of a nuclear power plant [2]. Currently, the average age of thermal power plants in Kazakhstan is 61 years, and about 76% of them have been operating for more than 50 years [3]. Despite concerns about nuclear energy, Kazakhstan may face electricity shortages without building new power plants, since most thermal plants are outdated. To prevent future energy shortages, it is necessary to implement energy consumption forecasting systems.

Every year, forecasting systems become more accurate, but they are still under development. Currently, there is no model that can perfectly predict electricity consumption for a city or a country. Forecasting models must consider many factors such as temperature,

humidity, time, and other external variables, since these factors directly influence electricity demand.

At the early stage of energy consumption forecasting, simple models such as Linear Regression, Random Forest, and Support Vector Machines (SVM) were widely used. These models showed good results in short-term forecasting when the data was well prepared [4]–[9]. Later, neural networks significantly improved forecasting performance. Models such as Long Short-Term Memory (LSTM) and Convolutional Neural Networks (CNN) became popular [4], [6], [10]–[15]. These models can capture dependencies between variables such as energy consumption and temperature. However, their complexity increased, and they require more computational resources. Distributed systems made it possible to process millions of records from smart meters for forecasting tasks [16].

Recently, transformer-based architectures such as Patchformer and PatchTST have shown highly accurate results in time series forecasting [17]–[19]. These models are able to capture both short-term and long-term dependencies.

Although significant progress has been made, many models still have limitations. Simple models like Linear Regression and SVM work well only when the dataset is small and relationships between variables are simple. They perform poorly with seasonal fluctuations, nonlinear relationships, and weather conditions [5], [7]–[9].

Even advanced neural networks such as LSTM and CNN have some limitations:

- They require significant computational resources and long training time [4].
- They often work as “black box” models, making interpretation difficult [11], [12].
- LSTM models are effective for short-term forecasting but may lose accuracy in long-term predictions [10].

In many studies, weather data is added only as additional features without modeling interactions between variables. Because of this, models may not fully capture complex dependencies, which reduces forecasting accuracy. In addition, many models perform poorly for long-term forecasting horizons, which limits their practical use [4], [16], [20].

In this study, we use the PatchTST model, which is based on a transformer architecture. A key feature of PatchTST is patch-level representation, which allows the model to capture both local and global temporal dependencies. The model uses 90 days of historical energy consumption data to forecast the next 14 days.

The forecasting results can help monitor changes in energy demand and support decision-making, such as adjusting the operation of thermal power plants to avoid unnecessary resource consumption.

The public dataset “Smart Meters in London” from Kaggle was used to train the model [21]. This dataset contains household energy consumption data as well as weather information, which can be integrated into the forecasting model.

In the future, Kazakhstan may widely adopt smart meters in cities and districts to collect energy consumption data. In that case, models like PatchTST could be applied to predict national energy demand. Currently, we use the Smart Meters in London dataset to improve the model so that it requires fewer computational resources while being able to make longer-term forecasts, potentially for several months ahead, in order to anticipate possible energy shortages.

## **Methodology**

### ***PatchTST Model Architecture Design***

To predict electricity consumption, we used the modern PatchTST model based on transformer architecture, which was introduced in 2023. A key feature of this model is its ability to identify relationships in time series data, even when these relationships are not obvious. PatchTST performs better than traditional models because it can learn complex dependencies between variables more effectively. It also shows higher accuracy when the relationships between data points are nonlinear and influenced by multiple factors.

The working principle of the model can be explained with a simple example. Imagine a calendar: the model divides the time series into small segments called “patches,” similar to splitting a calendar into groups of days. The model then learns how these patches are connected to each other over time.

In addition, external parameters such as weather conditions can be included in the model. For example, the model can learn that electricity consumption usually increases during cold weather and decreases during warm weather. This ability allows PatchTST to capture both temporal patterns and the influence of external factors.

### ***Dataset Preparation***

To train the model, we used an open dataset from Kaggle [21], which contains daily electricity consumption data for 5,567 households in London, along with weather parameters. The data was collected from January 2012 to March 2014.

The energy consumption dataset includes aggregated daily electricity usage for each household. For each day, the dataset provides statistical indicators such as average, median, minimum, and maximum consumption values, as well as other related measurements. A more detailed description of the dataset is presented in Table 1.

**Table 1 - Description of electricity consumption dataset fields**

| Field Name    | Description                                                              |
|---------------|--------------------------------------------------------------------------|
| LCLid         | Unique identifier for each smart meter/house.                            |
| day           | The calendar date (YYYY-MM-DD) of the aggregated consumption data.       |
| energy median | The median electricity consumption in kWh.                               |
| energy mean   | The average electricity consumption in kWh.                              |
| energy max    | The maximum electricity consumption in kWh.                              |
| energy count  | The number of measurements.                                              |
| energy std    | The standard deviation of the electricity consumption in kWh.            |
| energy sum    | The total electricity consumption in kWh summed across all measurements. |
| energy min    | The minimum electricity consumption in kWh.                              |

The weather dataset contains aggregated daily weather indicators corresponding to the households. For each day, the dataset provides statistics such as maximum and minimum temperature, humidity, wind speed, wind direction, cloud coverage, and other weather-related information. A more detailed description of the weather parameters is presented in Table 2.

**Table 2 - Description of weather dataset fields**

| Field Name     | Description                                                          |
|----------------|----------------------------------------------------------------------|
| time           | Timestamp of the recorded weather data (in Unix format or datetime). |
| temperatureMax | Maximum temperature (°C) for the day.                                |
| temperatureMin | Minimum temperature (°C) for the day.                                |

|                 |                                                              |
|-----------------|--------------------------------------------------------------|
| temperatureHigh | High temperature recorded during the day.                    |
| temperatureLow  | Low temperature recorded during the day.                     |
| humidity        | Relative humidity as a fraction from 0 to 1.                 |
| dewPoint        | Dew point temperature (°C), indicating atmospheric moisture. |
| windSpeed       | Wind speed (m/s).                                            |
| windBearing     | Wind direction in degrees (0–360).                           |
| cloudCover      | Fraction of sky covered by clouds (0–1).                     |
| pressure        | Atmospheric pressure (hPa).                                  |
| visibility      | Visibility distance in kilometers.                           |
| precipType      | Type of precipitation (e.g., rain, snow, sleet).             |

Figure 1 shows the dynamics of total daily electricity consumption over the entire observation period. It can be observed that weather conditions play an important role in electricity demand. Energy consumption increases during the winter months and decreases during the summer months.

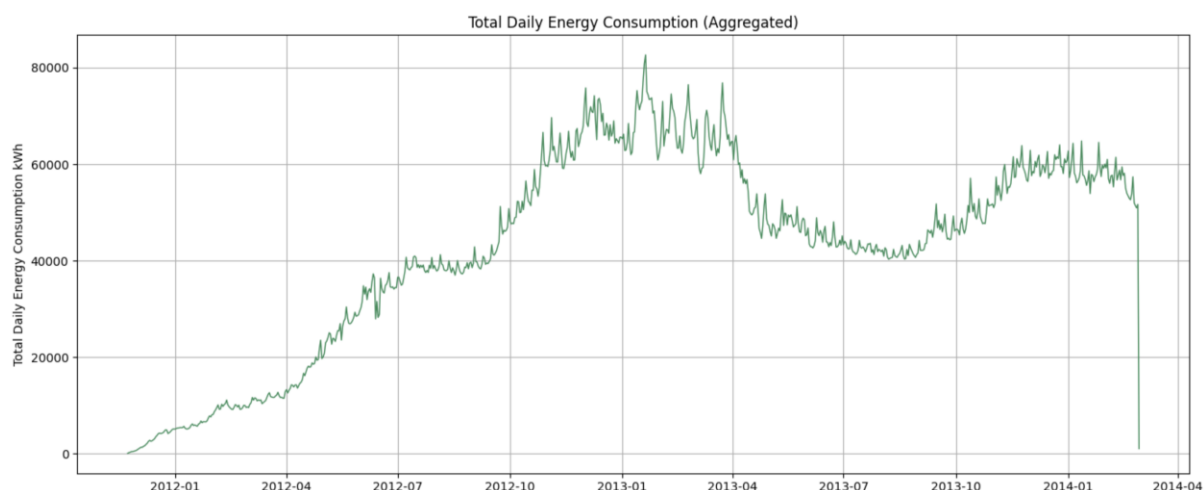


Fig. 1 - Graph of total daily energy consumption for the period from 2012 to 2014.

### **Implementation and Training**

The Smart Meters in London dataset was used to train the PatchTST model. This dataset contains daily electricity consumption data along with weather parameters. The data was preprocessed to reduce noise and simplify the input features.

The model was trained using three years of data. Approximately 80% of the dataset was used for training, and the remaining 20% was used for testing.

The training process followed a sliding window approach: the model used 90 days of historical energy consumption as input and predicted electricity consumption for the next 14 days. The model was trained for 10 epochs and achieved good performance, as shown in Table 3. Root Mean Square Error (RMSE) was used as the evaluation metric. RMSE measures the difference between predicted values and actual values, allowing us to assess the accuracy of the model.

**Table 3 - Training progress over 10 epochs**

| Epoch | Average Loss (RMSE) | Training time (sec) |
|-------|---------------------|---------------------|
| 1     | 0.01147             | 306.45              |

|    |         |        |
|----|---------|--------|
| 2  | 0.00449 | 333.20 |
| 3  | 0.00377 | 308.64 |
| 4  | 0.00351 | 323.70 |
| 5  | 0.00336 | 313.11 |
| 6  | 0.00327 | 336.71 |
| 7  | 0.00319 | 342.13 |
| 8  | 0.00313 | 336.89 |
| 9  | 0.00307 | 327.05 |
| 10 | 0.00303 | 352.88 |

**Results.** In this study, the PatchTST model was used to predict energy consumption. The model takes 90 days of historical energy consumption and weather data as input and forecasts electricity consumption for the next 14 days. Figure 2 presents the testing results of the model. Using 90 days of input data, the model generated a 14-day energy consumption forecast.

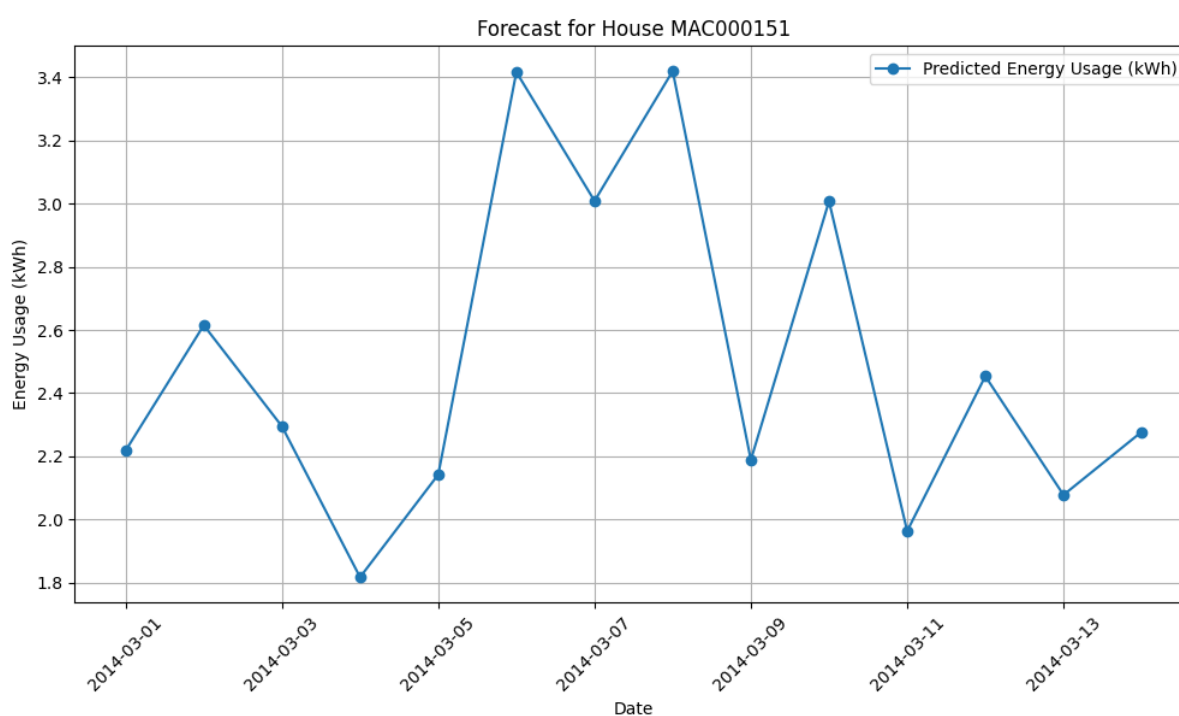


Fig. 2 - 14-day Energy Consumption Forecasting

Compared to models presented in other studies, our model achieved significantly better RMSE results. For example, in [16], a Random Forest model was trained, showing RMSE values ranging from 0.0945 to 0.2201. In [7], KNN and SVM models were trained, achieving RMSE values of 0.0125 and 0.0108, respectively. In [5], the SVR model achieved an RMSE value of 0.8. In contrast, our PatchTST model achieved an RMSE value of 0.003, which indicates much higher forecasting accuracy.

Although the PatchTST model demonstrated strong performance, it still has some limitations. Currently, the model predicts up to 14 days ahead, which is sufficient for short-term forecasting. However, it could be improved to generate forecasts for longer periods, such as several months ahead. In addition, the model was trained using daily energy consumption data. If hourly data were used, it would allow for more detailed analysis and potentially improve forecasting performance.

In this paper, the PatchTST model was trained for short-term forecasting of electricity consumption using time series and weather data from the dataset. The performance of PatchTST was significantly better than that of other models, including STM and similar approaches.

**Conclusion.** In this paper, the PatchTST model was trained for short-term forecasting of electricity consumption using time series and weather data from the dataset. The performance of PatchTST was significantly better than that of other models, including Random Forest, KNN, SVM, SVR, and similar approaches.

The use of PatchTST showed a low error rate, demonstrating that this model is well-suited for predicting energy consumption influenced by weather conditions. The patch-based approach allows the model to capture both local and global patterns, which accelerates training and improves accuracy. This makes PatchTST effective for both short- and long-term forecasting tasks.

Despite its strong performance, the PatchTST model has some limitations. First, training the model requires significant computational resources when processing large datasets. Second, like other transformer-based models, its interpretability is relatively low, functioning as a “black box,” which makes it difficult to explain the predictions. Additionally, preparing and assembling large datasets for training and forecasting can be resource-intensive.

In the future, the prediction horizon of the PatchTST model could be extended, and real-time forecasting capabilities could be added. Long-term forecasts could help prevent electricity shortages. Currently, in some cities, power outages still occur for several hours or even days. A real-time energy consumption prediction tool in Kazakhstan could help mitigate these electricity shortages and improve energy management.

### References:

1. Mitsubishi Research Institute, “How japan can deal with ai energy demand,” <https://www.mri.co.jp/en/knowledge/article/2024081.html>, 2024.
2. Kazakhstan Institute for Strategic Studies (KISI), “Public support for nuclear power plants grows in kazakhstan — survey,” <https://kisi.kz/ru/v-kazahstane-rastet-chislo-storonnikov-aes-sochopros/>, 2024.
3. TASS. (2023) In kazakhstan, it was stated that the average age of power plants in the country exceeds 60 years. <https://tass.ru/ekonomika/16439829>.
4. T. H. D. Mai, C. K. Leung, J. Lu, N. Giesbrecht, and O. A. Hnylycia, “A data science solution to integrate weather data for energy consumption analysis,” in Proceedings - 2024 IEEE International Conference on Information Reuse and Integration for Data Science, IRI 2024. Institute of Electrical and Electronics Engineers Inc., 2024, pp. 69–75.
5. H. Haque, A. K. Chowdhury, M. N. R. Khan, and M. A. Razzak, “Demand analysis of energy consumption in a residential apartment using machine learning,” in 2021 IEEE International IOT, Electronics and Mechatronics Conference, IEMTRONICS 2021 - Proceedings. Institute of Electrical and Electronics Engineers Inc., 4 2021.
6. C. Zongo, F. T. Ouedraogo, and S. Malo, “Forecasting models for monthly energy consumption using machine learning in burkina faso,” in IEEE AFRICON Conference. Institute of Electrical and Electronics Engineers Inc., 2023.
7. D. A. Bashawyah and S. M. Qaisar, “Machine learning based short-term load forecasting for smart meter energy consumption data in london households,” in 2021 IEEE 12th International Conference on Electronics and Information Technologies, ELIT 2021 - Proceedings. Institute of Electrical and Electronics Engineers Inc., 2021, pp. 99–102.

8. P. Vijayan, "Energy consumption prediction in low energy buildings using machine learning and artificial intelligence for energy efficiency," in 2022 8th International Youth Conference on Energy, IYCE 2022. Institute of Electrical and Electronics Engineers Inc., 2022.
9. A. Vartholomaios, S. Karlos, E. Kouloumpiris, and G. Tsoumakas, "Short-term renewable energy forecasting in greece using prophet decomposition and tree-based ensembles," 7 2021. [Online]. Available: <http://arxiv.org/abs/2107.03825>
10. D. L. Marino, K. Amarasinghe, and M. Manic, "Building energy load forecasting using deep neural networks," Tech. Rep., 2016.
11. A. V. Abraham, P. Sasidharan, S. J. Tejas, M. Manohara, R. Muthu, and R. C. Naidu, "Predicting energy consumption using lstm and cnn deep learning algorithm," in 2022 7th International Conference on Environment Friendly Energies and Applications: Renewable and Sustainable Energy Systems, Hybrid Transportation Systems, Energy Transition, and Energy Security, EFEA 2022 - Proceedings. Institute of Electrical and Electronics Engineers Inc., 2022.
12. R. Rane, M. Desai, A. Pandey, and F. Kazi, "Energy consumption forecasting using a deep learning energy-level based prediction," in 2021 IEEE International Power and Renewable Energy Conference, IPRECON 2021. Institute of Electrical and Electronics Engineers Inc., 2021.
13. X. Chen, T. Guo, M. Kriegel, and P. Geyer, "A hybrid-model approach for reducing the performance gap in building energy forecasting," 5 2022. [Online]. Available: <https://arxiv.org/abs/2206.00460>
14. J. Dumas, A. W. D. Lanaspeze, B. Corn'elusse, and A. Sutura, "A deep generative model for probabilistic energy forecasting in power systems: normalizing flows," 6 2021. [Online]. Available: <http://arxiv.org/abs/2106.09370>
15. D. Kaur, S. N. Islam, A. Mahmud, E. Haque, and Z. Y. Dong, "Energy forecasting in smart grid systems: Recent advancements in probabilistic deep learning," 2015. [Online]. Available: [www.ietdl.org](http://www.ietdl.org)
16. C. Dong, L. Du, F. Ji, Z. Song, Y. Zheng, A. Howard, P. Intrevado, and D. Woodbridge, "Forecasting smart meter energy usage using distributed systems and machine learning," in Proceedings - 20th International Conference on High Performance Computing and Communications, 16th International Conference on Smart City and 4th International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2018. Institute of Electrical and Electronics Engineers Inc., 1 2019, pp. 1293–1298.
17. Q. Hong, F. Meng, and F. Maldonado, "Advancing long-term multi-energy load forecasting with patchformer: A patch and transformer-based approach," 4 2024. [Online]. Available: <http://arxiv.org/abs/2404.10458>
18. C. Wang, P. Pinson, and Y. Wang, "Seamless and multi-resolution energy forecasting," 12 2023. [Online]. Available: <http://arxiv.org/abs/2401.05413>
19. A. Moradi, M. Tanneau, R. Zandehshahvar, and P. V. Hentenryck, "Enhanced renewable energy forecasting and operations through probabilistic forecast aggregation," 2 2025. [Online]. Available: <http://arxiv.org/abs/2502.07010>
20. J. 'Angel Gonz'alez Ordiano, L. Gr'oll, R. Mikut, and V. Hagenmeyer, "Probabilistic energy forecasting using quantile regressions based on a new nearest neighbors quantile filter," 3 2019. [Online]. Available: <http://arxiv.org/abs/1903.07390>
21. J.-M. Deveau, "Smart meters in london," <https://www.kaggle.com/datasets/jeanmidev/smart-meters-in-london>, 2020.

УДК 347.1

**Бақытбекқызы Анар**

Магистрант 2 курса, «MIS», каф. ПИ  
КазННТУ имени К. И. Сатпаева  
(г. Алматы, Казахстан)

## **ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ ОБРАЗОВАТЕЛЬНЫХ ПЛАТФОРМ (MOODLE, BLACKBOARD, GOOGLE CLASSROOM) И РАЗРАБОТКА СТРАТЕГИИ ЗАЩИТЫ ДАННЫХ**

**Аннотация:** В статье представлен системный анализ уязвимостей распространённых образовательных платформ дистанционного обучения — Moodle, Blackboard и Google Classroom — с позиции современных угроз информационной безопасности. Особое внимание уделено рискам, связанным с обработкой персональных данных обучающихся и преподавателей, интеграцией сторонних сервисов и облачной инфраструктурой.

**Ключевые слова:** образовательные платформы, Moodle, Blackboard, Google Classroom, информационная безопасность, уязвимости, защита данных, персональные данные, веб-безопасность, аутентификация, контроль доступа, утечки информации, инциденты ИБ, облачные сервисы.

Целью данной статьи является исследование уязвимостей платформ Moodle, Blackboard и Google Classroom, а также разработка стратегии защиты данных, учитывающей современные угрозы и особенности эксплуатации систем дистанционного обучения.

Архитектурные особенности образовательных платформ Moodle Moodle представляет собой веб-ориентированную модульную платформу с открытым исходным кодом, которая может развертываться как в локальной инфраструктуре образовательной организации, так и в частном или публичном облаке. Архитектура платформы включает веб-сервер приложений, сервер баз данных, файловое хранилище, а также подсистему расширений и плагинов.

Основным источником рисков безопасности Moodle является гибкая система расширений, позволяющая подключать сторонние модули, которые нередко разрабатываются без соблюдения требований безопасного программирования.

Архитектура Blackboard платформы относится к классу коммерческих LMS-решений и ориентирована на использование в крупных образовательных учреждениях. Система поддерживает сложную ролевую модель, масштабируемую архитектуру и интеграцию с внешними сервисами аналитики, прокторинга и управления идентификацией.

На рисунке 1 представлена упрощённая архитектура платформы Blackboard, демонстрирующая распределённую структуру сервисов и наличие множества точек интеграции, каждая из которых может выступать потенциальным вектором атаки.

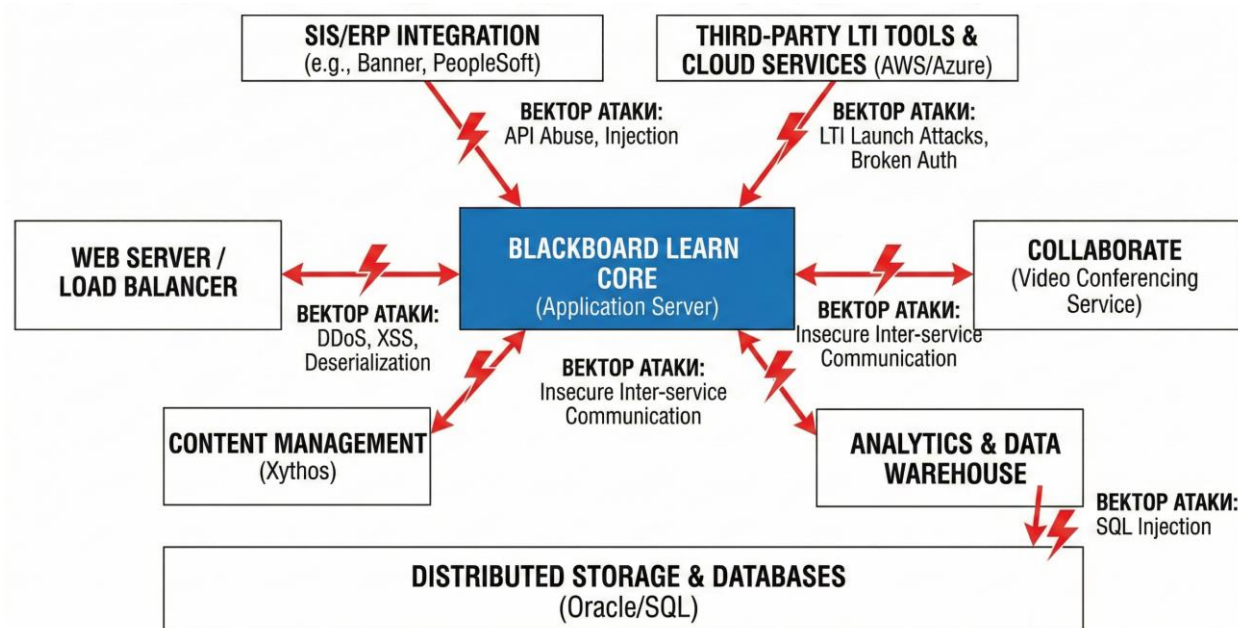


Рис. 1 – Архитектура платформы Blackboard с указанием на потенциальный вектор атаки

Как показано на рисунке 1, платформа Blackboard построена на основе распределённой архитектуры сервисов, взаимодействующих между собой через внутренние и внешние интерфейсы. Наличие большого числа интеграционных точек, включая модули управления курсами и внешние сервисы, увеличивает поверхность атаки и требует усиленного контроля безопасности при настройке доступа и обмене данными.

Архитектура Google Classroom функционирует как облачный сервис и является частью экосистемы Google Workspace. Аутентификация и управление доступом осуществляются через учетные записи Google, а хранение данных реализовано в распределённой облачной инфраструктуре.

На рисунке 2 показана модель взаимодействия пользователей с Google Classroom и связанными сервисами Google, отражающая основные потоки данных и зависимость безопасности платформы от политик облачного провайдера.

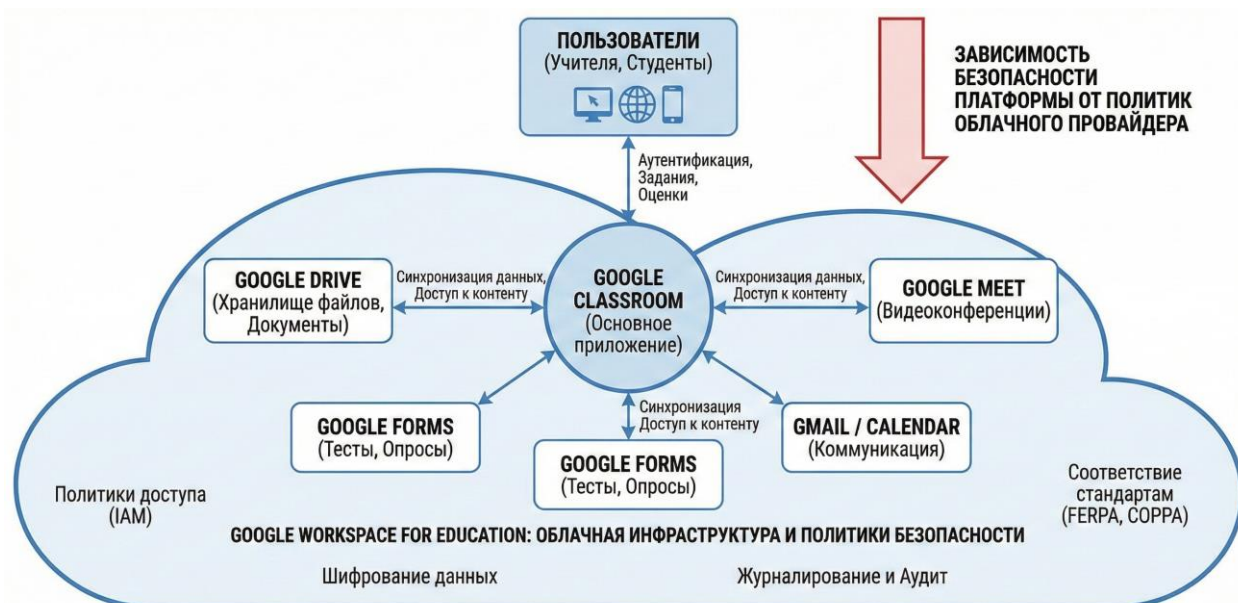


Рис. 2 – Модель взаимодействия пользователей с Google Classroom

Как показано на рисунке 2, платформа Google Classroom функционирует в тесной интеграции с облачными сервисами Google, что определяет основные потоки данных между пользователями и инфраструктурой провайдера. Безопасность платформы в значительной степени зависит от корректности настройки облачных политик доступа, управления учетными записями и защиты API, через которые осуществляется взаимодействие между компонентами системы.

Уязвимости веб-приложений и плагинов эти платформы Moodle и Blackboard подвержены классическим уязвимостям веб-приложений, таким как межсайтовый скриптинг, SQL-инъекции и подделка межсайтовых запросов. Особую опасность представляют уязвимости в сторонних плагинов и модулях расширения.

На рисунке 3 показаны основные потоки персональных данных в образовательной платформе и точки потенциальной утечки информации.

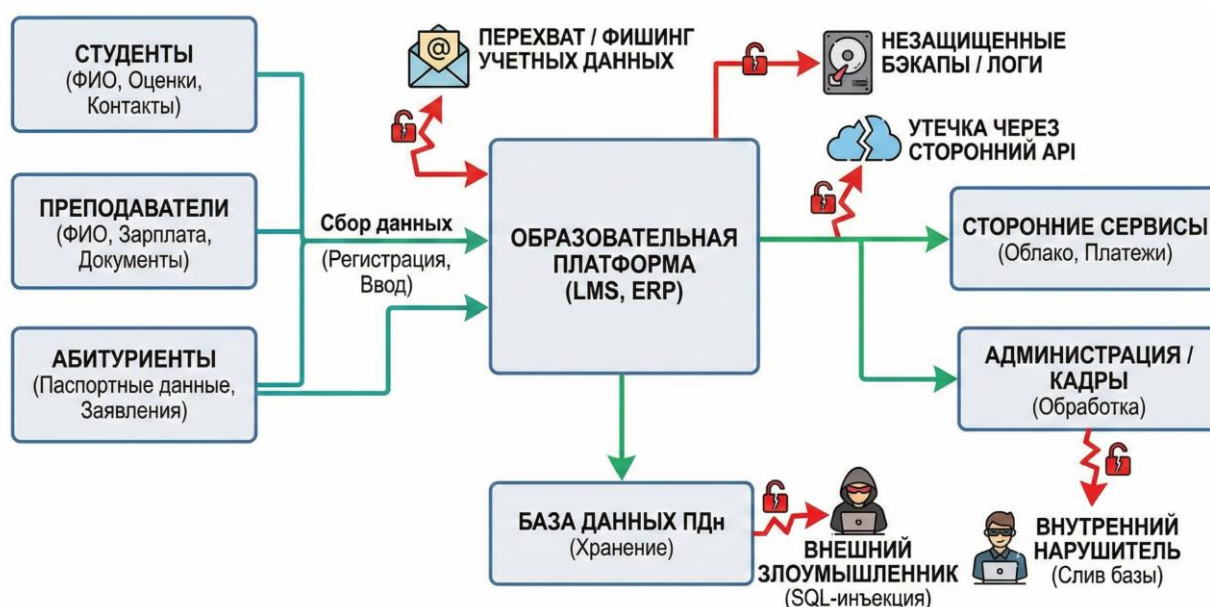


Рис. 3 – Основные потоки персональных данных

Как показано на рисунке 3, персональные данные пользователей циркулируют между основными компонентами образовательной платформы, включая пользовательские интерфейсы, сервер приложений, базы данных и внешние сервисы. Наличие нескольких точек передачи и хранения данных формирует потенциальные зоны утечки информации, что требует применения мер защиты на всех этапах обработки данных.

На рисунке 4 представлена архитектура защищённой образовательной платформы с интеграцией средств мониторинга и обнаружения атак.

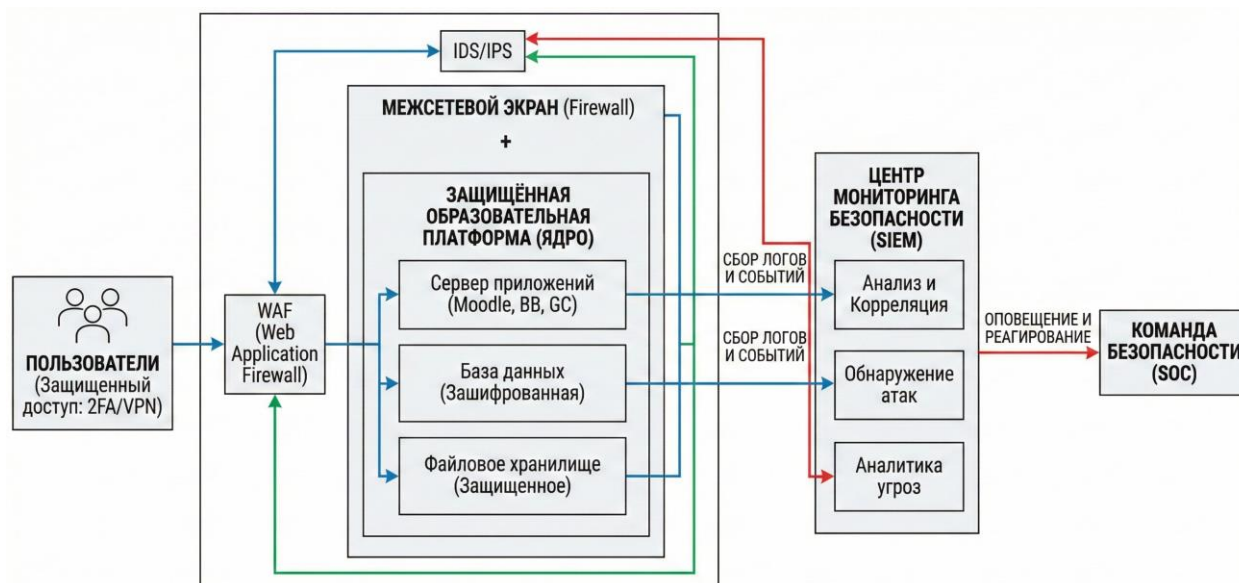


Рис. 4 – Архитектура защищённой образовательной платформы

Как показано на рисунке 4, защищённая образовательная платформа включает интеграцию средств мониторинга, систем обнаружения атак и управления доступом. Такая архитектура позволяет контролировать ключевые точки взаимодействия пользователей с системой, своевременно выявлять аномальные события и снижать риски несанкционированного доступа и утечки данных.

В статье проведено комплексное исследование уязвимостей образовательных платформ Moodle, Blackboard и Google Classroom и разработана стратегия защиты данных, учитывающая современные угрозы информационной безопасности. Реализация предложенных мер позволяет повысить уровень защищённости систем дистанционного обучения и обеспечить сохранность персональных данных пользователей.

### Список литературы:

1. Яламов Г. Ю. О современном состоянии обучения кибербезопасности // Вестник МГПУ. Серия: Информатика и информатизация образования. 2020. № 3 (53). С. 52–60. DOI 10.25688/2072-9014.2020.53.3.06.
2. Датаев А. А., Калитин Н. С., Харченко С. Б. Угрозы и вызовы кибербезопасности в онлайн-образовании // Проблемы современного педагогического образования. 2024. № 83-3. С. 144–147.
3. Магомадова А. Р., Айгулов Т. Г., Синицин А. М. Развитие кибербезопасности в образовательной среде: защита данных и личной информации // Проблемы современного педагогического образования. 2024. № 83-3. С. 273–276.
4. Кокорев Н. М. Безопасность в условиях цифровых коммуникаций учащихся // Актуальные проблемы безопасности в техносфере. 2023. № 3 (11). С. 6–9. DOI 10.34987/2712-9233.2023.99.67.001.
5. Эпова А. В. Кибербуллинг и его воздействие на психическое состояние // Интеллектуальные ресурсы - региональному развитию. 2024. № 1. С. 415–420.
6. Сыкеев Д. В., Сыкеева И. Н. Проблемы обеспечения информационной безопасности // Актуальные проблемы гуманитарных и социально-экономических наук. 2023. № 4 (100). С. 45–48.

7. Польченко М. А. Анализ рисков в информационной среде // Молодой исследователь Дона. 2023. Т. 8. № 3 (42). С. 55–62.

8. Войкова Н. А. Мошенничество в Сети: получение конфиденциальной информации посредством фишинга // Вестник Российско-Армянского (Славянского) университета: гуманитарные и общественные науки. 2022. № 4 (43). С. 46–54. DOI 10.48200/1829-0450\_sh\_2022\_4\_46.

9. Бронникова Н. А. Ресурсы цифровой платформы «Дневник. ру»: пути повышения эффективности управления образованием // Преемственность в образовании. 2021. № 28. С. 503–510.

UDC 004.94:37.091.3

**Zhakhangir Temir**

Master's Student, Computer Science and Engineering,  
Astana IT University  
(Astana, Kazakhstan)

**Symbat Nurgaliyeva**

PhD in Computer Science, Assistant Professor,  
Astana IT University  
(Astana, Kazakhstan)

## **A COMPARATIVE REVIEW OF THE ARCHITECTURE AND APPLICATION METHODS OF OPEN-SOURCE SIMULATORS FOR TEACHING ROBOTICS AND IOT**

**Abstract:** The need for scalable and accessible simulation environments has grown as robotics and Internet of Things (IoT) technologies are incorporated into engineering education. Open-source robotics simulators support middleware-enabled deployment and reproducible experimentation, making them an affordable substitute for hardware-based labs. The architectural design and educational uses of four popular simulators—Gazebo, Webots, CoppeliaSim, and MORSE—are compared in this paper. Modular architecture, sensor modeling, middleware compatibility, physics engine integration, and scalability are all examined. Although programmable control interfaces and physics-based modeling are the foundation of all four platforms, their usability, configurability, and instructional suitability vary. Webots facilitates introductory robotics education, MORSE allows reproducible multi-robot experimentation, and Gazebo and CoppeliaSim complement advanced and research-focused courses. The review offers structured guidance for selecting simulation tools in robotics and IoT curricula.

**Key words:** robotics simulation, IoT education, Gazebo, Webots, CoppeliaSim, MORSE, ROS, educational robotics

**Background and Significance.** Simulation technologies allow for cost-effective, scalable, and repeatable experimentation without solely depending on physical hardware infrastructures, they have become essential to modern robotics and Internet of Things (IoT) education [1, 2]. The need for secure and manageable virtual environments where students can investigate kinematics, control algorithms, perception pipelines, and networked device interactions has increased due to the growing complexity of cyber-physical systems and distributed sensor networks [3, 4]. In robotics education in particular, simulators help close the so-called "reality gap" between simulation and physical execution by mitigating hardware constraints, lowering maintenance costs, and enabling quick iterations of control strategies before deployment on real systems [5, 6]. Likewise, simulation facilitates experimentation with sensor data collection, communication protocols, and embodied interactions within cyber-physical systems in IoT-focused curricula [4, 7]. Furthermore, by facilitating continuity between virtual experimentation and actual robotic

platforms, the integration of robotics simulators with middleware frameworks like ROS has enhanced the pedagogical value of simulation [8, 9]. As blended and remote learning models continue to expand, simulation-based environments have proven particularly effective in maintaining practical engagement in distributed educational contexts [10].

**Purpose and Scope.** The purpose of this literature review is to examine and comparatively analyze four prominent open-source (or academically accessible) robotics simulators—Gazebo, Webots, CoppeliaSim, and MORSE—in the context of robotics and IoT education. While numerous simulation frameworks and supporting technologies exist [11, 3], this review focuses specifically on these four platforms due to their documented use in educational and research settings [1, 6]. Supporting technologies including physics engines (e.g., ODE, Bullet, PhysX), middleware such as ROS, and educational platforms like EUROPA or MOOC-based simulation integrations—are discussed only insofar as they influence simulator architecture or pedagogical application (Erez et al., 2015; Bertrand et al., 2019; Karalekas et al., 2020) [9, 12, 13]. This review attempts to give educators and researchers a systematic understanding of how simulator selection affects curriculum design, instructional methodology, and experimental reproducibility by examining architectural design, integration capabilities, pedagogical applications, and comparative performance characteristics.

**Overview of Open-Source Simulators.** Open-source simulators play a significant role in education focused on robotics and Internet of Things (IoT) due to cost-effective, repeatable, and scalable experimentation without dependence on physical hardware. These simulators allow educators and researchers to inspect internal models, extend functionality, and align simulation environments with specific curricular or research requirements [1, 13]. In the context of robotics and IoT education, this literature review focuses on four open-source robotics simulators: Gazebo, Webots, CoppeliaSim (formerly V-REP), and MORSE. Other systems and frameworks—such as ROS, physics engines (e.g., ODE, Bullet, PhysX), and educational platforms (e.g., EUROPA, DroMOOC)—are treated as supporting technologies that might be used alongside a certain simulator or as an internal component.

Overall, reviewed simulators rely on a physics engine to model real-world dynamics and interactions, provide mechanisms for robot construction and environment definition, and support programmable control through scripting or external interfaces. Additionally, reviewed simulators integrate with auxiliary tools and frameworks notably - Robot Operating System (ROS) that is described later in this paper. Gazebo is primarily adopted in academic and research settings where close alignment with real robotic systems is required, as its architecture supports detailed physical modeling, complex sensor configurations, and the use of external frameworks [6, 14]. Webots, by contrast, prioritizes an integrated development workflow, combining a graphical modeling environment with ready-to-use robot descriptions and controllers, which reduces setup overhead and supports structured learning in introductory and intermediate robotics courses [15, 16]. CoppeliaSim distinguishes itself through a distributed control paradigm and extensive API support, allowing control logic to be implemented via embedded scripts or external processes, which facilitates experimentation with multi-robot coordination and cyber-physical system architectures [6, 17]. MORSE adopts a scripting-first design centered on Python-based configuration and execution, favoring reproducibility and deterministic experimentation over graphical richness, and is therefore particularly suited to research-oriented and methodology-driven educational use cases [14]. To add to their base functionality, these simulators not only support the simulation of robot kinematics and dynamics but also enable the integration of IoT

components and protocols, providing an environment to explore the intersection of robotics and IoT systems [4]. The use of ROS as a middleware is common across these platforms, providing a standardized communication framework, therefore transferring progress from simulation dome to the real world [14, 18].

Educational applications of robotics simulators range from introductory programming and control courses to advanced research projects involving multi-robot coordination and IoT device integration. One of the examples is the EUROPA as a cost-effective ROS-based educational robot that teaches sensors, data acquisition, and robotics concepts with the help of simulation environments based on Gazebo and Python for scripting [9, 18]. Similarly, DroMOOC leverages simulation codes and experimental data sets within a MOOC framework to provide practical aerial robotics education remotely [13]. The growing adoption of open-source simulators in blended and online learning models reflects their adaptability and effectiveness in diverse educational contexts, providing hands-on learning experiences in remote or resource-constrained settings [4, 10]. In summary, open-source simulators serve as foundational tools in modern robotics and IoT education, offering scalable, extensible, and pedagogically rich environments that bridge theoretical knowledge and practical skills development.

**Architectural Features.** Open-source simulators for robotics and IoT education are characterized by several key architectural features that enable their flexibility, extensibility, and effectiveness in diverse educational contexts. These features include modular design, physics engine integration, middleware compatibility, and scalability.

*Core Components and Modular Design.* A defining characteristic of modern robotics simulators is their modular architecture, which separates core subsystems such as physics simulation, robot modeling, sensor abstraction, control interfaces, and visualization. This architectural separation supports curriculum scalability, allowing instructors to expose students gradually to increasing levels of system complexity [1]. Gazebo exemplifies this approach through its plugin-based architecture, enabling independent extension of sensors, actuators, controllers, and environmental dynamics [13]. CoppeliaSim similarly adopts a modular internal structure but extends it through embedded scripting and external APIs, enabling hybrid control strategies that combine local and remote computation [19]. Webots integrates most components within a unified development environment, trading some architectural openness for ease of configuration and reduced setup overhead [20]. MORSE emphasizes programmatic configuration via Python scripts, offering fine-grained control and reproducibility at the expense of graphical interactivity [21].

*Physics Engines and Sensor Simulation.* The realism of a robotics simulator is strongly influenced by its underlying **physics engine**, which governs rigid-body dynamics, collision detection, friction modeling, and sensor noise characteristics. Commonly used engines include ODE, Bullet, PhysX, and MuJoCo, each presenting trade-offs between numerical stability, computational cost, and physical fidelity [12]. Gazebo supports multiple physics engines (ODE, Bullet, DART, Simbody), enabling educators and researchers to adjust simulation fidelity based on instructional or experimental goals [22]. CoppeliaSim extends this flexibility by allowing runtime switching between Bullet, ODE, Newton, and Vortex, facilitating comparative studies of engine behavior under identical scenarios [19]. Webots relies exclusively on ODE, prioritizing determinism and simplicity over configurability [20]. MORSE uses Bullet via the Blender game engine, focusing on consistency and reproducibility rather than high-end physical realism [21]. Sensor simulation across these platforms typically includes cameras, LiDAR, IMUs, GPS, and

range sensors, enabling realistic perception pipelines essential for both robotics and IoT-oriented curricula.

*Integration with Robotics Middleware (e.g., ROS).* Integration with robotics middleware—most notably ROS—is a critical architectural feature that enables code portability between simulation and physical hardware. Gazebo and Webots provide native ROS integration, allowing students to deploy identical ROS nodes in simulated and real environments [9]. CoppeliaSim and MORSE support ROS through dedicated interfaces and middleware bridges, enabling similar workflows with additional configuration effort [19, 21]. This middleware compatibility is pedagogically significant, as it supports project-based learning models in which simulation serves as a precursor to real-world deployment.

*Scalability and Extensibility.* Open-source simulators are designed to scale from simple single-robot scenarios to complex multi-robot and IoT system simulations. Their extensible architectures support adding new robot models, sensors, and IoT devices, as well as custom scripting and programming interfaces in languages like Python, C++, and Lua [4, 14]. This scalability allows educators to adapt the simulators for various educational levels and research purposes, from introductory courses to advanced projects involving distributed robotic systems.

In summary, the architectural features of open-source simulators emphasize modularity, realistic physics simulation, middleware integration, and scalability, which collectively support their widespread adoption in robotics and IoT education.

**Application Methods in Educational Contexts.** Open-source simulators have been widely adopted in educational contexts to facilitate teaching and learning of robotics and IoT concepts through interactive, hands-on experiences. Simulation-based teaching approaches leverage these platforms to provide students with safe, cost-effective environments where they can experiment with robot programming, control algorithms, and IoT device integration without the constraints of physical hardware [1, 10]. Gazebo, Webots, and CoppeliaSim are widely used to teach kinematics, dynamics, control, and perception. Platforms such as EUROPA demonstrate how ROS-based simulators can be integrated into structured curricula to teach sensing and data acquisition [9]. DroMOOC illustrates how simulation environments can support large-scale, remote robotics education through MOOCs [13]. In IoT-oriented courses, robotics simulators facilitate experimentation with sensor networks, data flows, and cyber-physical interactions [4]. While network simulators such as NS-3 and OMNeT++ are often used for protocol-level studies, robotics simulators provide complementary system-level perspectives by modeling embodied sensing and actuation. Hybrid and blended learning models increasingly rely on simulators to support asynchronous experimentation and remote access. Empirical studies indicate that such models improve engagement and learning outcomes when simulations are aligned with clearly defined learning objectives [10].

Overall, the application of open-source simulators in educational contexts spans a wide range of methodologies and use cases, from introductory programming to advanced research projects, and from robotics-specific courses to interdisciplinary IoT education. Their adaptability and effectiveness make them indispensable tools in modern STEM education.

**Comparative Analysis.** The comparative analysis in this review explicitly concerns Gazebo, Webots, CoppeliaSim, and MORSE. Supporting tools such as ROS, physics engines, and educational platforms are discussed only insofar as they influence simulator capabilities. Open-source simulators for robotics and IoT education each present unique strengths and limitations that influence their suitability for different educational contexts.

*Gazebo* is widely recognized for its robust physics simulation and extensive integration with the Robot Operating System (ROS), offering high fidelity and realism but with a steeper learning curve and higher computational demands [1, 6]. From an architectural standpoint, *Gazebo* supports multiple physics engines—including ODE, Bullet, DART, and Simbody—allowing educators and researchers to adjust simulation fidelity and computational performance according to instructional needs [22]. Its native support for URDF and SDF models further facilitates seamless transitions between simulated and real robotic platforms [22].

*Webots*, in contrast, provides a more user-friendly interface and faster setup, making it particularly accessible for beginners and rapid prototyping, though it may lack some advanced features available in *Gazebo* [15, 16]. According to its official documentation, *Webots* relies exclusively on the Open Dynamics Engine (ODE) for physics simulation and offers built-in support for a wide range of sensors and actuators commonly used in mobile robotics, such as cameras, LiDAR, GPS, and inertial measurement units [20]. *Webots* also supports programming in C/C++, Python, and Java, enabling flexibility in pedagogical settings while maintaining a relatively shallow learning curve [20].

*CoppeliaSim* (formerly V-REP) stands out for its versatile programming support and distributed control architecture, enabling complex multi-robot and IoT system simulations, but its breadth of features can challenge novice users [6, 17]. Official documentation indicates that *CoppeliaSim* supports multiple physics engines—namely Bullet, ODE, Newton, and Vortex—which can be switched within the same simulation environment to compare performance and accuracy trade-offs [19]. In addition, *CoppeliaSim* offers multiple control modalities, including embedded Lua scripts, remote APIs, ROS interfaces, and external client programs, making it particularly suitable for advanced experimentation in distributed and heterogeneous robotic systems [19].

*MORSE* provides a lightweight and extensible simulation platform primarily aimed at multi-robot research and education, with an emphasis on script-based configuration rather than graphical scene editing [14]. According to its documentation, *MORSE* is built on top of the Blender game engine and uses Bullet as its underlying physics engine, with robots, sensors, and environments defined programmatically using Python [21]. While this design supports reproducibility and fine-grained control, it offers fewer built-in models and less graphical interactivity than *Gazebo*, *Webots*, or *CoppeliaSim*, which may limit its appeal in introductory educational contexts [6].

Performance and accuracy considerations across these simulators are closely tied to their underlying physics engines and numerical solvers. Benchmark studies comparing engines such as Bullet, ODE, and PhysX demonstrate inherent trade-offs between computational efficiency, contact stability, and physical realism, which directly influence simulation outcomes in educational and research settings [12]. *Gazebo*'s configurable engine support and *CoppeliaSim*'s multi-engine architecture provide greater flexibility in addressing these trade-offs, whereas *Webots* and *MORSE* are more constrained due to their reliance on a single physics engine [20, 21]. However, usability and learning curve vary significantly among the simulators. *Webots* and *MORSE* are generally more approachable for beginners due to their streamlined interfaces and scripting workflows, respectively, whereas *Gazebo* and *CoppeliaSim* demand more advanced technical skills but offer greater extensibility and realism [1, 6]. These differences directly affect their adoption in educational settings, particularly when balancing instructional time against desired simulation fidelity. Community support and documentation further influence educational

adoption. Gazebo and Webots benefit from large, active user communities and comprehensive official tutorials, reference manuals, and example repositories [20, 22]. CoppeliaSim's community is growing, supported by detailed official documentation and example scenes, while MORSE maintains a smaller but specialized user base focused on research-oriented applications [9, 13, 19, 21].

In summary, the choice of simulator should align with educational objectives, student expertise, and available computational resources. Gazebo and CoppeliaSim are well suited for advanced courses emphasizing realism, ROS integration, and extensibility; Webots is particularly effective for introductory robotics and rapid prototyping; and MORSE supports specialized, script-driven multi-robot experimentation. Balancing realism, usability, and extensibility is therefore essential to maximizing learning outcomes in robotics and IoT education.

**Identified research gaps.** Current literature predominantly evaluates robotics simulators from technical or performance perspectives, with limited empirical investigation into their impact on learning outcomes, curriculum design, and mitigation of the reality gap in educational settings. Comparative pedagogical frameworks remain underdeveloped. Emerging research focuses on hybrid simulation–hardware learning models, cloud-based and high-performance simulation infrastructures, reinforcement learning integration, and tighter coupling between robotics and IoT ecosystems. Future work should examine measurable educational effectiveness and develop standardized evaluation criteria for simulator selection in academic contexts.

**Conclusion.** This review analyzed the architectural foundations and educational applications of four open-source robotics simulators—Gazebo, Webots, CoppeliaSim, and MORSE—in robotics and IoT education. Although differing in design philosophy, all rely on physics-based modeling, programmable control interfaces, and integration with tools such as ROS. Gazebo and CoppeliaSim offer high configurability and realism, supporting advanced coursework and research-oriented experimentation. Webots provides an accessible and integrated development environment suited for introductory education, while MORSE emphasizes scripting and reproducibility for controlled multi-robot studies. From a pedagogical standpoint, these simulators enable scalable experimentation and alignment between simulated and real robotic systems, particularly in hybrid and resource-constrained learning environments. Simulator selection should therefore reflect instructional objectives, student expertise, and available resources rather than feature richness alone. Future research should further explore the relationship between simulator realism, learning outcomes, and mitigation of the reality gap.

### References:

1. Tselegkaridis S., Sapounidis T. Simulators in Educational Robotics: A review // *Education Sciences*. 2021. Vol. 11, № 1. P. 11.
2. Camargo C. et al. Systematic Literature Review of Realistic Simulators Applied in Educational Robotics context // *Sensors*. 2021. Vol. 21, № 12. P. 4031.
3. Collins J. et al. A review of Physics Simulators for Robotic Applications // *IEEE Access*. 2021. Vol. 9. P. 51416–51431.
4. Ciungan D.-A. et al. Enhancing IoT education through hybrid Robotic arm Integration: A quantitative and qualitative student experience study // *Applied Sciences*. 2025. Vol. 15, № 19. P. 10537.
5. Souza J.D.T. et al. Assessing the Reality Gap of Robotic Simulations with Educational Purposes. 2020. P. 1–6.

6. Farley A., Wang J., Marshall J.A. How to pick a mobile robot simulator: A quantitative comparison of CoppeliaSim, Gazebo, MORSE and Webots with a focus on accuracy of motion // *Simulation Modelling Practice and Theory*. 2022. Vol. 120. P. 102629.
7. Abdullah J. Simulation of wireless sensor networks (WSN) using NS-3 and OMNeT++ // *International Journal of Electronic Devices and Networking*. 2025. Vol. 6, № 1. P. 24–30.
8. Quigley M. ROS : an open-source Robot Operating System // *CiNii Research*. 2009.
9. Karalekas G., Vologiannidis S., Kalomiros J. EUROPA: A case study for teaching sensors, data acquisition and robotics via a ROS-Based Educational Robot // *Sensors*. 2020. Vol. 20, № 9. P. 2469.
10. Campos N. et al. Simulation-based education involving online and on-campus models in different European universities // *International Journal of Educational Technology in Higher Education*. 2020. Vol. 17, № 1.
11. Harris A., Conrad J.M. Survey of popular robotics simulators, frameworks, and toolkits. 2011. P. 243–249.
12. Erez T., Tassa Y., Todorov E. Simulation tools for model-based robotics: Comparison of Bullet, Havok, MuJoCo, ODE and PhysX. 2015. P. 4397–4404.
13. Bertrand S. et al. Integrating Experimental Data Sets and Simulation Codes for Students into a MOOC on Aerial Robotics // *IFAC-PapersOnLine*. 2019. Vol. 52, № 9. P. 50–55.
14. Noori F.M. et al. On 3D simulators for multi-robot systems in ROS: MORSE or Gazebo? 2017. P. 19–24.
15. Michel O. Cyberbotics Ltd. WEBOTS™: Professional Mobile Robot Simulation // *International Journal of Advanced Robotic Systems*. 2004. Vol. 1, № 1.
16. De Melo M.S.P. et al. Analysis and Comparison of Robotics 3D Simulators. 2019. P. 242–251.
17. Zhang Y. et al. The application of CoppeliaSIM EDU in robot course teaching // *Journal of Education and Educational Research*. 2024. Vol. 7, № 1. P. 167–170.
18. Karalekas G., Vologiannidis S., Kalomiros J. EUROPA — A ROS-based Open Platform for Educational Robotics. 2019. P. 452–457.
19. CoppeliaSIM User Manual [Electronic resource]. URL: <https://manual.coppeliarobotics.com/> (accessed: 12.02.2025).
20. Cyberbotics: doc [Electronic resource]. URL: <https://cyberbotics.com/doc/guide/index> (accessed: 12.02.2025).
21. Overview — The MORSE Simulator documentation [Electronic resource]. URL: <https://www.openrobots.org/morse/doc/latest/morse.html> (accessed: 12.02.2025).
22. Gazebo Sim Architecture — Gazebo jetty documentation [Electronic resource]. URL: <https://gazebo.org/docs/latest/architecture/> (accessed: 12.02.2025).

UDC 004.891

**Kussaiyn Dinmukhamed**

Master's student  
Astana IT University  
(Astana, Kazakhstan)

**Zhumadillayeva Ainur**

Candidate of Technical Sciences, Associate  
Professor  
Astana IT University  
L.N. Gumilyov Eurasian National University  
(Astana, Kazakhstan)

## **AI FACE RECOGNITION IN CROWDED PLACES: CHALLENGES, DIFFICULTIES, AND COMPARATIVE ANALYSIS**

**Abstract.** This paper addresses the challenges and difficulties encountered in the use of AI-based facial recognition systems in a variety of real-world environments. The study focuses on several key factors that significantly affect the accuracy and overall performance of such systems, including variations in illumination, extreme or non-frontal viewing angles, partial occlusion of facial features, and the inherent diversity of demographic characteristics across different populations. These conditions create complex scenarios where even advanced models struggle to maintain consistent accuracy. Particular attention is paid to data privacy concerns and ethical issues, including algorithmic bias and the misuse of facial recognition technologies. The paper also examines different strategies for improving the robustness of algorithms under adverse conditions, such as the use of generative models for image reconstruction and the integration of transformers to handle diverse image contexts. Furthermore, a critical evaluation of current methodologies and technologies—such as CNNs, GANs, and ViTs—is presented, with a discussion of their individual advantages and limitations. The comparative insights provided in this work aim to support the development of more effective, reliable, and socially responsible AI systems. The results are intended to be useful for AI developers, computer vision researchers, and practitioners working in security and surveillance domains.

**Keywords:** face recognition; artificial intelligence; CNN; GAN; ViT; occlusion; lighting variation; real-time processing; ethical issues.

**Introduction.** Face recognition based on artificial intelligence (AI) has become important in recent advances in security, law enforcement, and public safety. Facial recognition systems (FRS) have been widely applied in identity identification and verification, access control, street clubs, and crime investigation. Their high accuracy and ability to automatically process large amounts of data make them indispensable in modern settings, especially in crowded cities and at public events.

However, despite impressive advances in machine learning and neural network storage, the implementation of FRS in crowded spaces faces technical and ethical challenges. One of the main challenges is partial face occlusion caused by crowds. In a crowd, faces can be covered by other people, accessories (e.g., masks, glasses, hats) or objects, which significantly complicates identification (Valeriani & Poli, 2019).

Another important challenge is lighting variability. Unlike in a laboratory setting, where lighting is controlled, in a field it can change depending on the time of day, weather conditions and the location of light sources. This affects the accuracy of the models, since the same faces can look different in different lighting conditions (Santoso, Safitri & Samidi, 2024).

In addition, in crowded areas, there is a problem of scalability and computational load. Processing a large number of people at first requires significant computing resources. Modern deep learning algorithms such as convolutional neural networks (CNNs) and transformer models can improve the accuracy of the results, but they require powerful hardware, which limits their application in real-time settings (Zhao et al., 2020).

An equally important aspect is the ethical and legal side of using FRS in catering establishments. External systems of these financial issues related to personal privacy are associated with misuse of technology, as well as the risks of algorithmic bias (Buolamwini & Gebru, 2018). Misidentification can lead to serious consequences, especially if the system is used in relevant authorities.

Therefore, the use of AI-based FRS in crowded settings remains a serious challenge that requires addressing technical, computational and ethical issues. This article will provide an overview of current methods and algorithms, their impact on solving these problems, a comparative analysis of their effectiveness, as well as a discussion of key metrics and an outlook for future research.

**Literature Review.** Application of artificial intelligence (AI) for facial recognition is an emerging area that has found extensive application in areas such as security, surveillance, and identification. Yet, the performance of such systems in crowded scenes continues to be problematic because of occlusion, variation in lighting, computational resource limitations, and ethical concerns. Here, we talk about significant research on different elements of facial recognition in complicated scenarios.

### ***Facial Recognition Algorithms and Models***

Contemporary face recognition technology is based on advanced deep neural network architectures, including convolutional neural networks (CNNs), transformers, and hybrid models. According to research by Zhao et al. (2020), CNNs are still the most applied approach because of their capacity to extract intricate features from images at high identification accuracy. In congested settings, however, the performance of these models decreases because of issues such as perspective variations, occlusions, and image noise. Another approach includes transformer models, which utilize attention mechanisms to improve the accuracy of image inspection. Wang et al. (2023) proposed the Vision Transformer (ViT) architecture, designed to improve facial recognition performance in changing environments, and showed a reduction in recognition errors of partially occluded faces. However, such models require massive computational resources, and its application to real-time scenarios is made challenging.

### ***Impact of Occlusion and Variability in Conditions***

One of the key challenges is partial occlusion of faces by other objects. Valeriani & Poli (2019) analyzed how occlusion affects recognition algorithm accuracy and concluded that

existing models show a sharp decline in performance when more than 30% of the face is obscured. They proposed a combined approach, integrating information from multiple frames and predicting missing image regions using generative adversarial networks (GANs). Lighting variability also plays a significant role. Research by Santoso, Safitri, and Samidi (2024) showed that models trained in laboratory conditions significantly lose accuracy in real-world scenarios with varying lighting. As a solution, the authors proposed adaptive image preprocessing and lighting normalization methods.

### ***Computational Constraints and Real-Time Performance***

The use of complex neural network models requires powerful hardware, especially in crowded environments where hundreds of faces must be processed simultaneously. Singh et al. (2022) proposed model optimization based on weight quantization and pruning, which reduced computational load without significantly compromising accuracy. Additionally, cloud technologies and edge computing are being actively explored to reduce processing delays. Research by Li et al. (2021) demonstrated that distributed computing between local devices and cloud servers achieves a balance between accuracy and system speed.

### ***Ethical and Legal Challenges***

Applications using facial recognition technologies have generated questions regarding data privacy and the possibility of algorithmic bias. Buolamwini and Gebru (2018) demonstrated that current commercial algorithms are more accurate for light-skinned men than for women and darker-skinned subjects, potentially generating discriminatory outcomes. The situation questions whether greater diversity is needed in datasets and whether facial recognition systems need to be regulated. Marda & Singh's (2023) study discussed the legal side of the utilization of facial recognition in public areas and identified that there are stringent limitations in certain areas, including the European Union. In other parts of the world, including China and the United States, facial recognition technologies continue to be developed and implemented in law enforcement and business fields.

### ***Contemporary Facial Recognition Algorithms***

#### ***Convolutional Neural Networks (CNNs)***

Convolutional Neural Networks (CNNs) for Facial Recognition Convolutional neural networks (CNNs) are still a foundation of contemporary face recognition systems. Their power is in extracting spatial hierarchical features efficiently, which has been crucial for applications such as face identification and verification in images and video sequences (Deng et al., 2020). Traditional architectures like FaceNet (Schroff et al., 2015) and DeepFace (Taigman et al., 2014) demonstrate the effectiveness of CNNs by generating dense facial embeddings that are comparable using distance measures. Nevertheless, in spite of their success, CNNs have remarkable limitations when utilized in crowded settings. Partially occluded faces or those exposed to atypical lighting conditions tend to be great challenges, resulting in decreased accuracy (Wang et al., 2021). This problem is especially pertinent to the subject of this research, since real-world applications often entail dense and dynamic crowds. Recent advances, including multi-scale CNNs and sophisticated data augmentation techniques, provide promising solutions, but their utility in large-scale, real-time settings still needs to be more thoroughly examined.

#### ***Computer Vision Transformers (ViTs)***

Recently, Vision Transformers (ViTs) have been introduced as a promising substitute for CNNs, and this is largely attributed to their self-attention mechanisms, which enable the capturing of global dependencies in images (Dosovitskiy et al., 2020). This makes them highly suitable for

face detection in challenging situations, e.g., in crowded public areas (Khan et al., 2022). A particular strength of ViTs is that they are resilient to lighting and angle changes, which usually degrade CNN performance. This flexibility would be extremely useful for practical crowd monitoring in the real world. However, their computational expense and requirement for large training datasets restrict their everyday applicability in real-time systems (Touvron et al., 2021). In light of the requirement for speedy processing in surveillance systems, research efforts should be directed towards streamlining ViT architectures for speed without sacrificing accuracy.

#### *Generative Adversarial Networks (GANs) for Image Enhancement*

Generative Adversarial Networks (GANs) are employed within facial recognition systems to enhance the quality of input images and restore missing details, especially in cases of poor lighting or partial occlusion (Goodfellow et al., 2014). Recent methods, including StyleGAN and its variants, allow for the generation of realistic images of faces and pre-enhancement of data before inputting it into recognition systems (Karras et al., 2021). The application of GANs alongside CNNs and ViTs substantially enhances the accuracy of facial recognition, particularly in noisy or low-quality images (Jiang et al., 2022). GANs are computationally expensive to train, making them less suitable for real-time application. GANs are computationally costly to train, which limits their real-time usage. Methodology Facial recognition technology using artificial intelligence (AI) in use today is being applied extensively in a broad range of security, access control, and open-space surveillance applications. Such systems are tremendously challenged, however, in crowded environments under varying lighting conditions, obstructions (beard, glasses, etc.) to the face, image manipulation, high density, and low capability to address real-time demands. This article examines fundamental practices and methodologies being adopted for increasing accuracy and reliability in facial recognition in challenging environments.

### **Methods for Face Detection and Recognition in Crowded and Low-Quality Environments**

#### *Face Detection and Verification Methods in Crowded Environments*

The face recognition process starts with face detection from an image or video stream. Recent detection techniques need to perform efficiently in busy backgrounds, multiple objects, and large variations of viewing angles.

#### *One-Stage and Multi-Stage Detection Methods*

One-stage face detectors, such as RetinaFace (Deng et al., 2020), provide high processing speed by using deep convolutional regression to predict facial locations. These models can detect faces even with significant variations in angle and scale. Multi-stage cascade methods involve multiple processing levels, starting with rapid identification of possible face regions and concluding with refined classification.

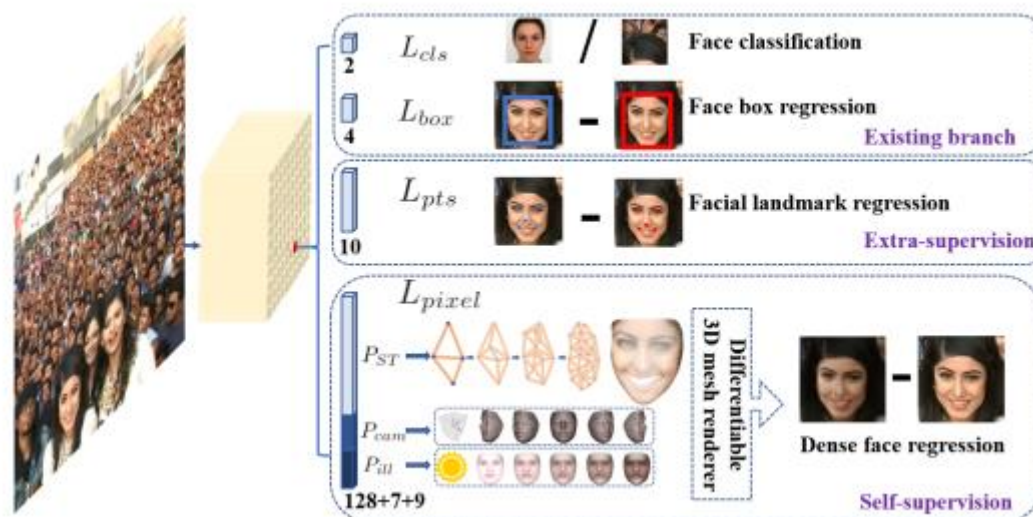


Figure 1 - A multi-branch architecture for face detection in crowded scenes with additional 3D face reconstruction. The combination of classification, bounding box regression, landmark prediction, and dense face regression improves accuracy under challenging conditions. (*Inspired by RetinaFace: Deng et al., 2019*)

## 1.2 Face Verification Methods

After detecting a face, verification is required to match it against a database. The following techniques are commonly used:

**Deep convolutional neural networks (CNNs)** extract high-level image features, allowing for highly accurate face classification.

**Transformers**, such as Vision Transformers (ViT) (Dosovitskiy et al., 2020), demonstrate high robustness to variations in lighting, angles, and backgrounds due to their self-attention mechanism.

## 2. Robustness to Occlusions and Lighting Variations

A major challenge in facial recognition systems is partial face occlusion by objects, people, or accessories (e.g., masks, glasses, scarves).

### 2.1 Generative Models for Recovering Occluded Facial Areas

**Generative adversarial networks (GANs)**, such as Alias-Free GAN (Karras et al., 2021), are used to reconstruct hidden facial regions. These models are trained on large datasets containing faces with varying degrees of occlusion, enabling the recovery of missing information.

### 2.2 Multi-Scale Convolutional Networks (Multi-Scale CNN)

**Multi-scale CNNs (Zhou et al., 2023)** analyze images at different levels of detail, improving face recognition performance in occluded conditions.

### 2.3 Adaptation Methods for Low-Light Conditions

**Deep neural architectures with image adaptation (Jiang et al., 2022)** enhance facial details in poor lighting conditions, improving input data quality before feeding them into the primary recognition model.

## 3. Application of Transformers and Ensemble Models for Facial Recognition

Traditional convolutional neural networks (CNNs) have limited capability for processing the global context of an image. To address this issue, transformers and ensemble models are increasingly being applied.

### 3.1 Vision Transformers (ViT) and Pyramid Vision Transformers (PVT)

**Pyramid Vision Transformer (Wang et al., 2021)** is an architecture that utilizes pyramid-based image processing, making it particularly useful for detecting faces in dense crowds.

### 3.2 Ensemble Methods for Improving Recognition Accuracy

**Ensemble models** combining CNNs and transformers help compensate for the shortcomings of each individual approach. For example, hybrid architectures that integrate CNNs for local analysis and transformers for global analysis lead to improved recognition accuracy.

### 4. Performance Evaluation Methods for Facial Recognition Systems

To objectively compare different algorithms, standardized metrics are used to assess their accuracy and reliability in real-world conditions.

#### 4.1 Key Accuracy Metrics for Recognition

**Precision, Recall, and F1-score** help evaluate how well the model classifies faces.

**False Acceptance Rate (FAR) and False Rejection Rate (FRR)** characterize the frequency of false acceptances and false rejections.

#### 4.2 Importance of Processing Speed

**Frames per second (FPS)** is a critical indicator for real-time applications, such as video surveillance systems.

### Comparative Analysis

Modern facial recognition algorithms vary significantly in terms of accuracy, computational efficiency, and robustness to external factors. The main approaches include convolutional neural networks (CNNs), transformers (ViTs), and generative adversarial networks (GANs), each with its own advantages and limitations.

#### 1. Accuracy and Robustness to Complex Conditions

CNNs remain the most popular solution due to their high accuracy on large datasets. However, their performance declines in the presence of occlusions and lighting variations. In contrast, ViTs demonstrate better robustness to these factors, as self-attention mechanisms allow for a holistic image analysis. GANs, in turn, are used for enhancing low-quality images, improving recognition results.

#### 2. Computational Costs and Real-Time Applicability

CNNs are optimized for real-time applications, particularly with mobile architectures such as . ViTs require more computational resources and processing time, making them less suitable for crowded, high-dynamic environments. GANs also have high computational complexity, especially during training, which limits their use in real-time monitoring systems.

#### 3. Scalability and Adaptability

CNNs scale well with sufficient data but require fine-tuning when operating conditions change. ViTs can process heterogeneous data and adapt to complex conditions but require large amounts of labeled images for training. GANs enable artificial dataset augmentation and image quality enhancement, but their stability and reproducibility remain challenging.

Thus, the choice of algorithm depends on the application conditions: CNNs remain the preferred solution for real-time tasks, ViTs perform better in complex environments, and GANs serve as a supplementary tool for data processing.

**Table 1 - Comparison of Popular Architectures (CNN, ViTs, GANs)**

| Architecture | Accuracy                                                    | Speed                                           | Noise Robustness                                     |
|--------------|-------------------------------------------------------------|-------------------------------------------------|------------------------------------------------------|
| CNN          | High (especially with sufficient data)                      | High (optimized implementations like MobileNet) | Medium (sensitive to occlusion and lighting changes) |
| ViTs         | Very High (outperforms CNNs with large datasets)            | Low (requires significant resources)            | High (ability to model global context)               |
| GANs         | Depends on application (mainly used as an auxiliary method) | Low (training requires powerful hardware)       | High (capable of restoring missing details)          |

Thus, the choice of architecture depends on the application conditions. For real-time applications, CNNs remain the preferred solution due to their speed, but for challenging conditions such as occlusion and lighting variations, ViTs and GANs are more appropriate at the expense of higher computational demands.

### **Obstacles and Constraints**

Despite the advancements in facial recognition systems, there remain significant challenges that hinder the seamless and widespread deployment of such systems in populous environments.

#### **1. Occlusion and Environmental Variability**

Interferences created by objects, individuals, or equipment, and changes in light and viewpoints drastically decrease the accuracy of recognition. Although existing models try to compensate for these influences, fully eliminating their impact is still a problem.

#### **2. Computational Resources**

Most advanced algorithms utilize significant computational resources, particularly if applied to large data streams in real-time. This limits the use of advanced architectures on low-power devices and necessitates hybridization with edge or cloud computing.

#### **3. Ethical and Legal Issues**

The use of facial recognition systems gives rise to large-scale debates in connection with privacy issues and rights protection for personal data. In some countries, their use is controlled by strict rules, while in others, there are no well-established legal frameworks, and such usage could potentially be used in abusive manners.

#### **4. Bias and Discrimination in Models**

Many algorithms exhibit varying degrees of accuracy across different demographic groups, which can lead to discrimination and false identification. Addressing this issue requires the development of more inclusive datasets and training methods that take into account facial heterogeneity.

Thus, the continual evolution of facial recognition technologies needs not only advancements in technical capabilities but also a deliberate consideration of the ethical and legal dimensions involved in their application.

### **Conclusion**

AI-powered facial recognition systems are developing further and being applied in security, access control, and surveillance of public spaces. Their use in crowded places raises

technical and ethical questions. This paper discussed some of the major concerns, such as occlusion, illumination variation, high computational requirement, and data privacy.

Modern algorithms, such as Convolutional Neural Networks (CNNs), Vision Transformers (ViTs), and Generative Adversarial Networks (GANs), have made significant progress in addressing these challenges. All proposed methods, however, come with their own limitations. CNNs are still known to be among the most reliable methods; they are, indeed, sensitive to imaging conditions' variations. On the contrary, ViTs have improved global image analysis capabilities but require extensive computational efforts. GANs assist in the restoration of missing information in images, yet their application in real time is restricted due to the extremely high training complexity.

Apart from technicality, regulatory and ethical issues also play a major role. A study emphasizes the need to work on clear-cut policies for applying facial recognition systems, protecting the data, and avoiding algorithmic bias. The regional variations in legal systems as well as general public attitudes toward such technologies are also important areas to be thought about.

In conclusion, although there has been tremendous advancement in AI-driven facial recognition, there remain some daunting challenges to overcome. Some of the avenues for future research involve developing more robust algorithms to external factors, reducing computational expenses, and creating fair and inclusive models. Overcoming these challenges will not only enable facial recognition systems to be more efficient and dependable but also guarantee that they are implemented ethically and responsibly in society.

### References:

1. Deng, J., Guo, J., Zhou, Y., Yu, J., Kotsia, I., & Zafeiriou, S. (2019, May 2). RetinaFace: Single-stage dense face localisation in the wild. arXiv.org. <https://arxiv.org/abs/1905.00641>
2. Dosovitskiy, A., Beyer, L., Kolesnikov, A., Weissenborn, D., Zhai, X., Unterthiner, T., Dehghani, M., Minderer, M., Heigold, G., Gelly, S., Uszkoreit, J., & Houlsby, N. (2020, October 22). An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale. arXiv.org. <https://arxiv.org/abs/2010.11929>
3. Khan, S., Naseer, M., Hayat, M., Zamir, S. W., Khan, F. S., & Shah, M. (2022). Transformers in Vision: a survey. ACM Computing Surveys, 54(10s), 1–41. <https://doi.org/10.1145/3505244>
4. Touvron, H., Cord, M., Douze, M., Massa, F., Sablayrolles, A., & Jégou, H. (2020, December 23). Training data-efficient image transformers & distillation through attention. arXiv.org. <https://arxiv.org/abs/2012.12877>
5. Wang, W., Xie, E., Li, X., Fan, D., Song, K., Liang, D., Lu, T., Luo, P., & Shao, L. (2021, February 24). Pyramid Vision Transformer: A Versatile Backbone for Dense Prediction without Convolutions. arXiv.org. <https://arxiv.org/abs/2102.12122>
6. Zeng, D., Veldhuis, R., & Spreeuwers, L. (2020). A survey of face recognition techniques under occlusion. arXiv (Cornell University). <https://doi.org/10.48550/arxiv.2006.11366>
7. Valeriani, D., & Poli, R. (2019). Cyborg groups enhance face recognition in crowded environments. PLoS ONE, 14(3), e0212935. <https://doi.org/10.1371/journal.pone.0212935>

8. Zhu, X., Su, W., Lu, L., Li, B., Wang, X., & Dai, J. (2020, October 8). Deformable DETR: Deformable transformers for End-to-End Object Detection. arXiv.org. <https://arxiv.org/abs/2010.04159>
9. Li, L., Mu, X., Li, S., & Peng, H. (2020). A review of face recognition technology. IEEE Access, 8, 139110–139120. <https://doi.org/10.1109/access.2020.3011028>
10. Jamil, S., Piran, M. J., & Kwon, O. (2023). A comprehensive survey of transformers for computer vision. Drones, 7(5), 287. <https://doi.org/10.3390/drones7050287>
11. William, I., Setiadi, D. R. I. M., Rachmawanto, E. H., Santoso, H. A., & Sari, C. A. (2019). Face Recognition using FaceNet (Survey, Performance Test, and Comparison). 2019 Fourth International Conference on Informatics and Computing (ICIC), 1–6. <https://ieeexplore.ieee.org/abstract/document/8985786>
12. Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., Santamaría, J., Fadhel, M. A., Al-Amidie, M., & Farhan, L. (2021). Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. Journal of Big Data, 8(1). <https://doi.org/10.1186/s40537-021-00444-8>
13. Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2017). ImageNet classification with deep convolutional neural networks. Communications of the ACM, 60(6), 84–90. <https://doi.org/10.1145/3065386>
14. Saxena, D., & Cao, J. (2021). Generative Adversarial Networks (GANs). ACM Computing Surveys, 54(3), 1–42. <https://doi.org/10.1145/3446374>
15. Karras, T., Aila, T., Laine, S., & Lehtinen, J. (2017, October 27). Progressive growing of GANs for improved quality, stability, and variation. arXiv.org. <https://arxiv.org/abs/1710.10196>
16. Salimans, T., Goodfellow, I., Zaremba, W., Cheung, V., Radford, A., & Chen, X. (2016, June 10). Improved techniques for training GANs. arXiv.org. <https://arxiv.org/abs/1606.03498>
17. Gu, J., Wang, Z., Kuen, J., Ma, L., Shahroudy, A., Shuai, B., Liu, T., Wang, X., Wang, L., Wang, G., Cai, J., & Chen, T. (2015, December 22). Recent advances in convolutional neural networks. arXiv.org. <https://arxiv.org/abs/1512.07108>
18. Kaur, P., Krishan, K., Sharma, S. K., & Kanchan, T. (2020). Facial-recognition algorithms: A literature review. Medicine Science and the Law, 60(2), 131–139. <https://doi.org/10.1177/0025802419893168>

УДК 621.316.1

Калиева Қарлығаш Бейсенбекқызы

магистрант 2 курса  
АО «Казахский агротехнический  
исследовательский университет им. С. Сейфуллина»  
(г. Астана, Казахстан)

## ПОВЫШЕНИЕ КОЭФФИЦИЕНТА МОЩНОСТИ СИСТЕМЫ ЭЛЕКТРОСНАБЖЕНИЯ ЗЕРНОВОГО ЭЛЕВАТОРА ТОО «БУЛАНДЫ-АСТЫК» С ПРИМЕНЕНИЕМ ЧАСТОТНЫХ ПРЕОБРАЗОВАТЕЛЕЙ

**Аннотация:** В статье рассматриваются вопросы повышения коэффициента мощности системы электроснабжения зернового элеватора ТОО «Буланды-Астык», расположенного в г. Макинске Акмолинской области Республики Казахстан. Проведён анализ электрических нагрузок предприятия, установлены причины низкого коэффициента мощности ( $\cos \varphi = 0,78-0,80$ ). Обоснована целесообразность применения частотных преобразователей (ЧП) на приводах конвейеров, норий, вентиляторов аспирации и зерносушилок как основного средства повышения  $\cos \varphi$  и снижения потребления реактивной мощности. Представлены результаты расчёта компенсирующих устройств — конденсаторных установок типа УКТ-0,38-150 суммарной мощностью 300 квар. Приведены технико-экономические показатели эффективности предложенных мероприятий, подтверждающие снижение потерь электроэнергии, уменьшение тока в питающих линиях и повышение  $\cos \varphi$  до 0,95–0,96.

**Ключевые слова:** коэффициент мощности, реактивная мощность, конденсаторная установка, частотный преобразователь, электроснабжение, зерновой элеватор, энергоэффективность.

**Введение.** Зерновые элеваторы относятся к числу предприятий агропромышленного комплекса с высокой долей электромеханических приводов в структуре потребителей электроэнергии. Многочисленные конвейеры, нории, вентиляторы аспирации, зерносушильные агрегаты, сепараторы и триеры, работающие на асинхронных электродвигателях, формируют значительную реактивную составляющую нагрузки. Следствием этого является низкий коэффициент мощности ( $\cos \varphi$ ) системы электроснабжения, который для большинства отечественных элеваторов не превышает 0,78–0,82, что существенно ниже нормируемого значения 0,92–0,95 [1].

Низкий  $\cos \varphi$  приводит к перегрузке питающих трансформаторов и кабельных линий реактивными токами, увеличению потерь активной мощности в элементах сети, снижению напряжения у потребителей, а также к штрафным санкциям со стороны энергоснабжающей организации за потребление реактивной мощности сверх установленных норм [2].

ТОО «Буланды-Астык» — один из крупнейших зерновых комплексов Акмолинской области, принимающий, сушащий, очищающий и хранящий зерно общей ёмкостью 18 000 тонн. Предприятие введено в эксплуатацию в 2008 году. В ходе его модернизации в 2020–2022 гг. был установлен ряд нового технологического оборудования фирмы Petkus

(предварительные очистители, модульные триеры, барабанные очистители), что повлекло рост суммарной электрической нагрузки и ещё большее снижение коэффициента мощности.

Настоящая статья посвящена анализу существующего состояния системы электроснабжения элеватора, обоснованию применения частотных преобразователей (ЧП) в качестве основного инструмента улучшения  $\cos \phi$ , а также расчёту параметров компенсирующих конденсаторных установок, обеспечивающих достижение нормируемых значений коэффициента мощности.

## **2 Характеристика объекта исследования**

### **2.1 Общие сведения о предприятии**

Элеватор ТОО «Буланды-Астык» расположен в г. Макинске Акмолинской области, вблизи железнодорожного узла, что обуславливает возможность приёмки зерна как автомобильным, так и железнодорожным транспортом. Климатические условия района характеризуются резко-континентальным климатом: абсолютный максимум температуры  $+42^{\circ}\text{C}$ , абсолютный минимум  $-47^{\circ}\text{C}$ , среднегодовая температура воздуха  $+6,1^{\circ}\text{C}$ . Расчётная температура наиболее холодной пятидневки составляет  $-35^{\circ}\text{C}$ . Среднегодовая продолжительность гроз — 60–70 часов; средняя скорость ветра — 15 м/с [3].

В состав производственного комплекса входят: рабочая башня — 1 ед.; автоприёмник — 1 ед.; автомобильные весы — 1 ед.; зерносушилка — 1 ед.; склады зерна — 2 ед.; силосный корпус — 5 ед.; железнодорожный приёмник — 1 ед.; лаборатория — 1 ед.; мельница — 1 ед.; мастерская — 1 ед.; гараж — 1 ед.; КПП — 1 ед.; трансформаторные подстанции (ТП) — 2 ед.

### **2.2 Технологический процесс и состав электрооборудования**

Технологический процесс элеватора включает следующие основные операции: приёмку зерна (взвешивание, отбор проб, первичная очистка), транспортировку по нориям и ленточным конвейерам, сушку до влажности 13–14,5 %, очистку на сепараторах и триерах, хранение в силосных корпусах с контролем температуры, отпуск потребителям.

Электрооборудование предприятия распределено по 12 распределительным пунктам (РП1–РП12). Суммарная установленная мощность электроприёмников силовой нагрузки составляет 1069,14 кВт. Преобладающими типами электроприёмников являются асинхронные электродвигатели с короткозамкнутым ротором мощностью от 0,25 до 75 кВт, работающие в длительном режиме.

Система электроснабжения предприятия выполнена по II категории надёжности. Питание осуществляется от подстанции 35/10 кВ «Элеватор» по двум воздушным линиям АС-35 длиной 3,2 км от фидеров №3 и №8. На территории предприятия установлены две трансформаторные подстанции 10/0,4 кВ с трансформаторами ТМ-630-10/0,4 (630 кВА каждый), работающими в параллельном режиме.

**Таблица 1 — Расчётные нагрузки по распределительным пунктам**

| Распределительный пункт | Наименование нагрузки                | $P_{\max}$ , кВт | $Q_{\max}$ , квар | $S_{\max}$ , кВА | $\cos \phi$ |
|-------------------------|--------------------------------------|------------------|-------------------|------------------|-------------|
| РП1                     | Рабочая башня (конвейеры, аспирация) | 76,44            | 45,03             | 88,71            | 0,862       |
| РП2                     | Нории №1–3, аспирация №5             | 143,84           | 92,77             | 171,24           | 0,840       |

| Распределительный пункт | Наименование нагрузки                     | $P_{\max}$ , кВт | $Q_{\max}$ , квар | $S_{\max}$ , кВА | $\cos \varphi$ |
|-------------------------|-------------------------------------------|------------------|-------------------|------------------|----------------|
| РПЗ                     | Конвейеры №5–12                           | 63,99            | 44,85             | 78,14            | 0,819          |
| РП4                     | Склады зерна (конвейеры, ысырмы)          | 28,06            | 18,96             | 33,86            | 0,829          |
| РП5                     | Силосный корпус (конвейеры, транспортёры) | 87,62            | 63,64             | 108,29           | 0,809          |
| РП6/6а                  | Галерейные конвейеры, тележки             | 52,33            | 33,73             | 62,26            | 0,840          |
| РП7                     | Зерносушилка (вентиляторы)                | 53,87            | 39,68             | 66,91            | 0,805          |
| РП8                     | Зерносушилка (транспортёры, вентиляторы)  | 95,37            | 70,25             | 118,45           | 0,805          |
| РП9                     | Автоприёмник (УРВС-15, Гуар-30)           | 49,65            | 35,93             | 61,28            | 0,810          |
| РП10                    | СОБ (очистители, триеры)                  | 57,16            | 46,16             | 73,48            | 0,778          |
| РП11                    | Мельница                                  | 38,46            | 26,96             | 46,96            | 0,819          |
| РП12                    | Мастерская                                | 11,72            | 11,24             | 16,24            | 0,722          |
| Итого                   | —                                         | 758,51           | 529,20            | 925,82           | 0,800          |

Из таблицы 1 видно, что коэффициент мощности по большинству распределительных пунктов находится в диапазоне 0,78–0,86, что не соответствует требованиям Правил устройства электроустановок (ПУЭ) и условиям договора с энергоснабжающей организацией, предписывающим поддерживать  $\cos \varphi$  не ниже 0,92 [4].

### 3 Анализ причин низкого коэффициента мощности

Основной причиной низкого  $\cos \varphi$  является преобладание в составе нагрузки асинхронных электродвигателей, потребляющих значительную реактивную мощность для намагничивания магнитной цепи. При этом существенным усугубляющим фактором является нерациональный режим работы электроприводов: значительная часть электродвигателей конвейеров, норий и вентиляторов работает в режиме неполной загрузки — на 40–70 % от номинальной мощности [5].

В условиях элеватора ТОО «Буланды-Астык» можно выделить следующие группы причин пониженного коэффициента мощности:

1) Работа асинхронных электродвигателей в режиме неполной нагрузки. Конвейеры и нории в период межсезонья или при неполной загрузке зерном работают на 40–60 % от номинала, что снижает  $\cos \varphi$  двигателя с 0,82–0,85 (при полной нагрузке) до 0,60–0,70 (при 50 % нагрузке).

2) Прямой пуск электродвигателей. При прямом пуске пусковой ток достигает 5–7-кратного значения от номинального, а  $\cos \varphi$  в пусковом режиме составляет 0,25–0,40. При

частых пусках (особенно в цехах первичной очистки) это существенно ухудшает средневзвешенный  $\cos \varphi$ .

3) Большое количество малонагруженного оборудования. Установленные ысырмы (заслонки) мощностью 0,25–0,55 кВт имеют крайне низкий коэффициент использования ( $K_i = 0,6$ ) и  $\cos \varphi = 0,70$ , что при их значительном количестве (18 шт.) суммарно вносит отрицательный вклад в общий  $\cos \varphi$ .

4) Неэффективный режим работы вентиляторов зерносушилок. Вентиляторы (изотермические, горячего и холодного продувания) с мощностями 18–30 кВт запускаются напрямую и работают на постоянной частоте вращения, не зависящей от фактической влажности и объёма зерна в сушилке. При этом реактивная мощность вентиляторного привода составляет 14,63–29,25 квар на единицу.

Суммарная реактивная мощность всех электроприёмников предприятия на шинах 0,4 кВ составила 533,4 квар при активной мощности 771,26 кВт, что соответствует  $\tan \varphi = 0,69$  и  $\cos \varphi = 0,82$ . С учётом потерь в трансформаторах суммарная реактивная нагрузка на шинах 10 кВ возрастает до 629 квар.

#### **4 Применение частотных преобразователей как метод повышения коэффициента мощности**

##### **4.1 Принцип действия и преимущества частотных преобразователей**

Частотный преобразователь (ЧП) — электронное устройство, изменяющее частоту и амплитуду напряжения питания асинхронного электродвигателя, обеспечивая тем самым плавное регулирование частоты вращения и крутящего момента. Современные ЧП серии ACS550, ACS800 (ABB), MICROMASTER 440 (Siemens), CIMR (Yaskawa) выполняются по схеме: выпрямитель → звено постоянного тока (конденсаторный фильтр) → инвертор (IGBT-транзисторы) [6].

Применительно к системе электроснабжения элеватора ЧП выполняют следующие функции:

— Улучшение коэффициента мощности на вводе. Современные ЧП с активным выпрямителем (AFE — Active Front End) обеспечивают  $\cos \varphi = 0,97–0,99$  на стороне питания, независимо от режима работы электродвигателя. Стандартные ЧП с диодным выпрямителем и LC-фильтром обеспечивают  $\cos \varphi = 0,93–0,96$  [7].

— Исключение реактивного тока намагничивания из питающей сети. При регулировании скорости ЧП потребляет из сети почти исключительно активную мощность, преобразуя её в мощность на валу двигателя, тогда как реактивная мощность циркулирует во внутреннем звене постоянного тока.

— Снижение потерь в двигателе и кабельных линиях. Регулирование скорости по законам  $U/f = \text{const}$  (скалярное) или с ориентацией по полю (векторное) позволяет поддерживать оптимальный поток в двигателе при частичной нагрузке, повышая КПД привода.

— Исключение пиков тока при пуске. Плавный пуск через ЧП ограничивает пусковой ток до 1,5–2  $I_n$ , что снижает провалы напряжения в сети и уменьшает реактивную составляющую при пуске.

##### **4.2 Выбор узлов для установки частотных преобразователей**

На основе анализа режимов работы электрооборудования элеватора и расчёта технико-экономической эффективности (соотношение срока окупаемости и годового

экономического эффекта) определены следующие приоритетные объекты для установки ЧП:

1) Вентиляторы зерносушилок (РП7, РП8): изотермический вентилятор 30 кВт, вентиляторы холодного и горячего продувания (15–30 кВт). Производительность зерносушилки варьируется в зависимости от влажности зерна и внешней температуры, однако без ЧП вентиляторы работают на постоянной скорости. Применение ЧП позволяет снизить потребление электроэнергии на 25–35 % при сохранении качества сушки.

2) Нории (РП2): нория №1–2 (2×38 кВт), нория №3 (75 кВт). Нории работают с переменной загрузкой в зависимости от интенсивности приёмки зерна. Установка ЧП обеспечивает регулирование скорости в диапазоне 50–100 % от номинала.

3) Вентиляторы аспирационных установок (РП1, РП3, РП6): аспирации №1–4 (4×15 кВт), №5 (22 кВт), №6–9 (4×1,1 кВт), №10 (11 кВт). Производительность аспирации можно регулировать в зависимости от запылённости воздуха, применяя частотно-регулируемый привод.

4) Конвейеры главного транспортного тракта (РП2, РП3): транспортёры с двигателями 10–17 кВт, работающие в режиме частичной загрузки при неполном заполнении зерна.

**Таблица 2 — Параметры частотных преобразователей для ключевых узлов элеватора**

| Объект установки         | Мощность ЭД, кВт | Тип ЧП (рекомендуемый) | Ожидаемый $\cos \phi$ на вводе | Снижение потребл. э/э, % |
|--------------------------|------------------|------------------------|--------------------------------|--------------------------|
| Нория №3 (РП2)           | 75               | ABB ACS550-01-157A-4   | 0,97                           | 15–20                    |
| Нории №1–2 (РП2)         | 2×38             | ABB ACS550-01-072A-4   | 0,97                           | 15–20                    |
| Изотерм. вент. (РП7)     | 30               | Siemens MM440 30кВт    | 0,96                           | 25–35                    |
| Вент. хол. продув. (РП8) | 22               | Siemens MM440 22кВт    | 0,96                           | 25–30                    |
| Вент. гор. продув. (РП8) | 30               | Siemens MM440 30кВт    | 0,96                           | 25–30                    |
| Аспирации №1–4 (РП1)     | 4×15             | Yaskawa CIMR-V 15кВт   | 0,95                           | 20–30                    |
| Конвейеры №8–9 (РП3)     | 2×15             | Yaskawa CIMR-V 15кВт   | 0,95                           | 15–20                    |

По результатам расчёта, установка ЧП на перечисленные электроприводы позволит снизить суммарное потребление реактивной мощности по предприятию с 533,4 квар до ориентировочно 340–360 квар, а  $\cos \phi$  на шинах 0,4 кВ — повысить с 0,80 до 0,87–0,89. Для достижения нормируемого значения  $\cos \phi = 0,95$  дополнительно требуется компенсация реактивной мощности с помощью конденсаторных установок.

## 5 Компенсация реактивной мощности конденсаторными установками

### 5.1 Расчёт мощности компенсирующего устройства

Требуемая мощность компенсирующей конденсаторной установки (КУ) определяется по формуле [8]:

$$Q_{ку} = \alpha \cdot P_{\max} \cdot (tg \varphi_p - tg \varphi_{tr}),$$

где  $\alpha$  — коэффициент, учитывающий несимметрию графика нагрузки ( $\alpha = 0,9$ );  $P_{\max} = 771,26$  кВт — расчётная максимальная активная мощность предприятия;  $tg \varphi_p = 0,69$  — расчётное значение  $tg \varphi$  по данным замеров;  $tg \varphi_{tr} = 0,33$  — требуемое значение  $tg \varphi$ , соответствующее  $\cos \varphi = 0,95$ .

$$Q_{ку} = 0,9 \cdot 771,26 \cdot (0,69 - 0,33) = 249,9 \text{ квар.}$$

С учётом дискретности выпускаемых конденсаторных установок принята к установке комплектная конденсаторная установка типа УКТ-0,38-150 в количестве 2 шт. суммарной мощностью 300 квар. Установки подключаются к шинам 0,4 кВ трансформаторных подстанций ТП-1 и ТП-2 по 150 квар на каждую.

### 5.2 Уточнённый расчёт коэффициента мощности после компенсации

После установки КУ суммарной мощностью 300 квар скомпенсированная реактивная мощность составит:

$$Q_p = Q_{\max} - Q_{ку} = 533,4 - 300 = 233,4 \text{ квар.}$$

Полная расчётная мощность с учётом компенсации:

$$S_p = \sqrt{(P_{\max}^2 + Q_p^2)} = \sqrt{(771,26^2 + 233,4^2)} = 805,0 \text{ кВА.}$$

Скомпенсированный коэффициент мощности:

$$\cos \varphi_p = P_{\max} / S_p = 771,26 / 805,0 = 0,958.$$

Полученное значение  $\cos \varphi = 0,96$  превышает нормируемый уровень 0,95 и соответствует требованиям договора электроснабжения. Загрузка трансформаторов ТМ-630-10/0,4 составит:

$$K_z = S_p / (n \cdot S_{ном}) = 805,0 / (2 \cdot 630) = 0,639.$$

Значение  $K_z = 0,64$  является оптимальным для двухтрансформаторной подстанции (рекомендуемый диапазон 0,6–0,75).

**Таблица 3 — Сравнение параметров системы до и после внедрения мероприятий**

| Параметр                            | До внедрения | После внедрения ЧП  | После ЧП + КУ    |
|-------------------------------------|--------------|---------------------|------------------|
| Активная мощность $P$ , кВт         | 771,26       | 748 (экон. ~23 кВт) | 748              |
| Реактивная мощность $Q$ , квар      | 533,4        | 360 (расчётно)      | 60–80 (нескомп.) |
| Полная мощность $S$ , кВА           | 925,8        | 830                 | 752              |
| Коэффициент мощности $\cos \varphi$ | 0,80         | 0,89                | 0,958            |
| Ток в линии 0,4 кВ, А (приб.)       | 1 414        | 1 267               | 1 145            |
| Загрузка трансформаторов $K_z$      | 0,735        | 0,659               | 0,599            |
| Потери в трансформаторах, кВт       | 8,12         | 6,51                | 5,53             |

## 6 Технико-экономическая эффективность

Расчёт экономической эффективности предлагаемых мероприятий выполнен на основе следующих исходных данных: тариф на электрическую энергию для промышленных предприятий Акмолинской области  $T_0 = 35,71$  тг/кВт·ч; число часов работы предприятия в год  $T_g = 5\,000$  ч; годовой штраф за потребление реактивной мощности сверх нормы (доплата за  $\text{tg } \varphi > 0,33$ ) — согласно действующей нормативно-правовой базе Республики Казахстан.

### **6.1 Экономия от снижения потерь в трансформаторах**

Снижение потерь активной мощности в трансформаторах после компенсации составит:

$$\Delta P_{\text{эк}} = P_{\text{потерь(до)}} - P_{\text{потерь(после)}} = 8,12 - 5,53 = 2,59 \text{ кВт.}$$

Годовая экономия электроэнергии за счёт снижения потерь в трансформаторах:

$$\Delta E_{\text{тр}} = \Delta P_{\text{эк}} \cdot T_g = 2,59 \cdot 5\,000 = 12\,950 \text{ кВт·ч/год.}$$

### **6.2. Экономия от применения частотных преобразователей**

Снижение потребления электроэнергии при установке ЧП на вентиляторы зерносушилок (закон изменения мощности для центробежных механизмов — кубичный в зависимости от скорости) при среднегодовом снижении скорости до 80 % от номинала составит:

$$P_{\text{ред}} = P_{\text{ном}} \cdot (n/n_{\text{ном}})^3 = P_{\text{ном}} \cdot 0,8^3 = 0,512 \cdot P_{\text{ном}}.$$

Суммарная установленная мощность вентиляторов зерносушилок:  $P_v = 30 + 15 + 22 + 30 + 18 = 115$  кВт. Экономия активной мощности при снижении скорости до 80 %:

$$\Delta P_v = 115 \cdot (1 - 0,512) = 56,1 \text{ кВт.}$$

Годовая экономия электроэнергии по вентиляторам (при  $T_r = 3\,000$  ч работы зерносушилок в год):

$$\Delta E_v = 56,1 \cdot 3\,000 = 168\,300 \text{ кВт·ч/год.}$$

### **6.3 Суммарный экономический эффект и срок окупаемости**

Суммарная годовая экономия электроэнергии:

$$\Delta E_{\text{сум}} = \Delta E_{\text{тр}} + \Delta E_v = 12\,950 + 168\,300 = 181\,250 \text{ кВт·ч/год.}$$

Годовой экономический эффект от снижения потребления электроэнергии:

$$Э_{\text{год}} = \Delta E_{\text{сум}} \cdot T_0 = 181\,250 \cdot 35,71 = 6\,472\,187 \text{ тг/год} \approx 6,47 \text{ млн тг/год.}$$

Капитальные затраты на приобретение и монтаж ЧП (7 единиц на ключевые узлы) и конденсаторных установок ( $2 \times \text{УКТ-0,38-150}$ ) ориентировочно составят:

— ЧП (7 ед. суммарной мощностью  $\approx 280$  кВт):  $K_{\text{чп}} \approx 8,5$  млн тг;

— Конденсаторные установки ( $2 \times \text{УКТ-0,38-150}$ ):  $K_{\text{кп}} \approx 0,9$  млн тг;

— Монтажные и пусконаладочные работы:  $K_{\text{монт}} \approx 1,2$  млн тг.

$K_{\text{общ}} = 8,5 + 0,9 + 1,2 = 10,6$  млн тг.

Простой срок окупаемости капиталовложений:

$$T_{\text{ок}} = K_{\text{общ}} / Э_{\text{год}} = 10,6 / 6,47 \approx 1,64 \text{ года.}$$

Срок окупаемости менее 2 лет является высокоэффективным показателем для энергосберегающих мероприятий в промышленности. Дополнительным экономическим эффектом является устранение штрафных санкций за потребление реактивной мощности сверх нормы и снижение платы за максимум нагрузки по двухставочному тарифу.

**Таблица 4 — Сводные технико-экономические показатели мероприятий**

| Наименование показателя           | Значение          | Единица измерения |
|-----------------------------------|-------------------|-------------------|
| Повышение $\cos \varphi$          | с 0,80 до 0,96    | —                 |
| Снижение реактивной мощности      | с 533,4 до ~60–80 | квар              |
| Годовая экономия электроэнергии   | 181 250           | кВт·ч/год         |
| Годовой экономический эффект      | 6,47              | млн тг/год        |
| Суммарные капитальные затраты     | 10,6              | млн тг            |
| Простой срок окупаемости          | 1,64              | лет               |
| Снижение потерь в трансформаторах | 32 %              | —                 |
| Снижение тока в питающих линиях   | 19 %              | —                 |

## 7 Обсуждение результатов

Полученные результаты согласуются с данными литературных источников о высокой эффективности применения ЧП на центробежных и подъёмно-транспортных механизмах агропромышленных предприятий. В работах Железко Ю.С. [9] и Мелентьева Л.А. [10] показано, что использование ЧП в системах вентиляции и транспортировки сыпучих материалов обеспечивает снижение потребления электроэнергии на 20–40 % при улучшении  $\cos \varphi$  до 0,95–0,99 в зависимости от типа преобразователя.

Специфика зерновых элеваторов состоит в сезонном характере загрузки: в период уборочной кампании (август–октябрь) нагрузка достигает 100 % от расчётной, а в межсезонье снижается до 30–50 %. Это предъявляет особые требования к регулированию конденсаторных установок: рекомендуется применение автоматически регулируемых КУ с тиристорными коммутаторами ступеней, обеспечивающих отключение части мощности при снижении нагрузки во избежание генерации реактивной мощности в сеть.

В отношении ЧП для норий следует отметить, что применение регулируемого привода требует предварительного анализа конструкции нории на предмет допустимости снижения скорости ленты: при уменьшении скорости ниже 60 % от номинальной возможно зависание зерна в ковшах. Поэтому диапазон регулирования рекомендуется ограничивать 70–100 % от номинала [11].

Суммарный эффект от комплексного применения ЧП и КУ ( $\cos \varphi = 0,96$ , срок окупаемости 1,64 года) существенно превосходит эффект от применения только КУ без ЧП ( $\cos \varphi = 0,96$ , но без экономии электроэнергии в самих приводах) и только ЧП без КУ ( $\cos \varphi \approx 0,89$ , что не достигает нормируемого уровня 0,95). Таким образом, комплексный подход является оптимальным.

**Заключение.** В результате проведённого исследования системы электроснабжения зернового элеватора ТОО «Буланды-Астык» установлено следующее:

1) Исходный коэффициент мощности предприятия составляет  $\cos \varphi = 0,80$ , что не соответствует нормируемым требованиям и обусловлено работой асинхронных электродвигателей конвейеров, норий, вентиляторов в режиме неполной нагрузки, а также значительным числом малонагруженных электроприёмников.

2) Предложен комплекс мероприятий по повышению коэффициента мощности, включающий: установку частотных преобразователей на приводы вентиляторов

зерносушилок (115 кВт), нории (151 кВт), аспирационные вентиляторы и конвейеры, а также установку двух компенсирующих конденсаторных установок УКТ-0,38-150 суммарной мощностью 300 квар на шинах 0,4 кВ трансформаторных подстанций.

3) Реализация предложенных мероприятий обеспечивает повышение  $\cos \varphi$  с 0,80 до 0,96, снижение реактивной мощности с 533 до 60–80 квар, уменьшение тока в питающих линиях на 19 %, снижение потерь мощности в трансформаторах на 32 %.

4) Годовая экономия электроэнергии составит 181 250 кВт·ч, годовой экономический эффект — 6,47 млн тенге при суммарных капитальных затратах 10,6 млн тенге. Простой срок окупаемости — 1,64 года, что подтверждает высокую инвестиционную привлекательность мероприятий.

5) Результаты исследования могут быть применены при разработке проектов реконструкции систем электроснабжения аналогичных зерновых предприятий Казахстана.

### Список литературы:

1. Правила устройства электроустановок (ПУЭ). — 7-е изд. — М.: Энергоатомиздат, 2003. — 648 с.
2. Железко Ю.С. Компенсация реактивной мощности и повышение качества электроэнергии. — М.: Энергоатомиздат, 1985. — 224 с.
3. СНиП РК 2.04-01-2017. Строительная климатология. — Астана: КазНИИИСА, 2017. — 136 с.
4. Технические условия на присоединение к электрической сети АО «КЕГОК». — Астана, 2022.
5. Онищенко Г.Б. Асинхронные электродвигатели в системах регулируемого электропривода. — М.: Энергоатомиздат, 2006. — 576 с.
6. Браун Т. Частотно-регулируемые приводы: теория и практика применения: пер. с англ. — М.: Техносфера, 2019. — 540 с.
7. Меньших О.Ф. Экономия электроэнергии в насосных и вентиляционных установках с частотно-регулируемым электроприводом // Промышленная энергетика. — 2010. — №4. — С. 35–41.
8. Идельчик В.И. Электрические системы и сети. — М.: Энергоатомиздат, 1990. — 592 с.
9. Железко Ю.С., Артемьев А.В., Савченко О.В. Расчёт, анализ и нормирование потерь электроэнергии в электрических сетях. — М.: ЭНАС, 2003. — 280 с.
10. Мелентьев Л.А. Системные исследования в энергетике. — М.: Наука, 1983. — 455 с.
11. Дегтярёв В.П., Редькин А.В. Эксплуатация зерноскладов и элеваторов. — М.: Агропромиздат, 1987. — 303 с.

ПАНДЕР АРАЛЫҚ ҒЫЛЫМДАР – МЕЖДИСЦИПЛИНАРНЫЕ НАУКИ –  
INTERDISCIPLINARY SCIENCES

UDC 81'23:81'27

Gazez Aishat Aibatkyzy

Master's student  
Maqsut Narikbayev University  
(Astana, Kazakhstan)

EMOTIONAL EXPRESSION IN TWO LANGUAGES: BILINGUAL PERSPECTIVES  
ON LANGUAGE CHOICE AND EMOTIONAL AUTHENTICITY

**Abstract:** Emotional expression is a fundamental aspect of human communication, forming social interactions and connections, perception, and cognitive processing. Bilingual individuals acquired two linguistic systems, which introduces complexity in the encoding, articulation, and perception of emotions. This review combines interdisciplinary research on emotional expression in bilingual contexts, highlighting factors such as language dominance, emotional authenticity, cognitive processing of emotion words, sociocultural norms, and communicative strategies, including code-switching. Scientific results demonstrate that emotional expressiveness is not solely determined by the first language acquired but is influenced by functional language use, contextual demands, and cultural frameworks. Findings underscore the context-sensitive nature of emotional expression in bilingual speakers across diverse linguistic and cultural settings.

**Keywords:** bilingualism, emotional expression, language choice, emotional authenticity, language dominance, code-switching.

The ability to experience and express emotions is a key aspect of communication, influencing subsequent interpretations, understanding and experience in social interactions. Each language has its own mechanism for encoding emotional expressions, when both bilinguals have two language systems that work together and sometimes it makes it difficult to express emotions clearly. In the context of emotional expression, the choice of language may depend not only on the level of language proficiency, but also includes other cognitive processes and socio-cultural environment that influence emotional experience and communication outcomes. [1]

Since then, research in the field of bilingualism and the expression of emotions has made significant progress, also considering various theories that include the fields of psycholinguistics, sociolinguistics, cognitive psychology and discourse, delving even deeper into this area from different perspectives. Earlier studies have argued that the expression of emotions is most closely related and depends on the first language, the one that was acquired in childhood, that is, the first, suggesting that the language of the first socialization in the world forms strong emotional associations, thereby emotional encoding, rather than languages acquired later. [2] However, more modern research often points to the dubiousness of this theory and examines such dynamic factors as language dominance, contextual use, cultural norms, and a person's personality. [3; 4]

This paper discusses the main results of interdisciplinary research on the expression of emotions in a bilingual context, where the main focus is on the most influential topics such as

emotional authenticity, cognitive processing of emotions and words, socio-cultural component, communicative practices in the form of code switching and innovations in methodologies. Thus, by studying current trends and identifying gaps in the existing literature, researchers in this field provide a comprehensive overview of how bilingual people express and perceive emotions in different languages and their features.

### **Language and Emotional Authenticity in Bilinguals**

#### ***Rethinking Emotional Primacy***

From the perspective of the traditional model of both bilingualism and emotions, it is most often assumed that the mother tongue, that is, the first language, has a special emotional value because of its significant role in the earliest human development and interaction within the family, in which the basis of emotionality is built. According to this theory, the expression of emotions in the first language is perceived as a more authentic expression of emotions compared to the language acquired later. [2] However, later empirical research in this area increasingly proves the dubiousness of this theory.

Studies based on autobiographical narratives confirm that the emotional intensity of a story depends not on the order of language proficiency, but on the dominance of language and the activity of its use by a person. For example, in a study with bilingual native speakers of English and Russian, more emotional expressions were used in a language that was comfortable for them in a certain context, regardless of which language they acquired first. [5] Thus, this confirms the idea that emotionality is associated with a comfortable and familiar language, and not just the primacy of language acquisition. [3]

Similarly, a study conducted in the context of native speakers of Persian-English showed in the results that emotional expressions, in particular negative ones, are easier to manifest in a second language, indicating a different emotional distance in languages and contexts. [6] These findings cast doubt on the idea that first language is the emotionally predominant language, demonstrating that emotional resonance strongly depends on linguistic usage in practice.

#### ***The Role of Language Dominance***

Language dominance is the relative level of language proficiency and the intensity of its use in practice in bilingual speech. Dominance does not depend on age or the order of language acquisition, it is gradually dynamically formed depending on the constant study of language, communication and the environment in society. [3] Modern research on bilinguals often claims that emotional attachment and expressiveness of emotions are determined by the dominance of the language rather than the status of the native or first language. [4]

Dominant languages evoke stronger emotionality and more accurate emotional description and expression. For example, in a study of balanced and unbalanced bilinguals, the results confirm that emotional comfort and the depth of emotional expression more often coincide with the dominant language, that is, with the most frequently used in everyday life, regardless of the order of language learning. [4] This pattern once again underscores the importance of the functional use of language in research on the expression of emotions of bilinguals.

Moreover, existing evidence of this sphere suggests that emotional authenticity is the subjective feeling that the expression of emotions feels more authentic and it depends on the context and can be formed from interaction rather than fixed attributes of a particular language.

[3] Thus, bilinguals can claim emotional authenticity in different languages, but depending on the social component, once again emphasizing the flexibility of using an “emotional” language.

## **Cognitive and Psycholinguistic Influences on Emotional Lexicon**

### ***Emotion and Cognitive Processing***

Beyond questions about the authenticity of emotional expression and the dominance of language, the researchers studied the expression of emotions of bilingual people from the prism of cognitive abilities and vocabulary. Conducting psycholinguistic experimental studies shows that emotionally charged expressions, especially vividly exciting or forbidden topics, awaken different cognitive processes depending on the language used at the moment. [6] As an example, according to the results of memory tasks, the memorization of emotional words is better in a language with which there is an association of strong emotional experiences or fragments. These results indicate a possible specific linguistic representation that affects the encoding and retrieval of information from human memory. [7]

The next indicator in research that confirms the special cognitive processes in different languages in the expression of emotions is the indicators of time and speed. The results of the conducted studies demonstrate differences in the speed of perception and processing of emotional and more neutral words in two languages among bilinguals. [6] Additionally, some results prove the influence of the dominant language on emotionality due to the speed of processing and reaction by the brain, which indeed indicates a strong neural connection between emotions and lexical expression. [9]

Going deeper into research on this topic from the neuro-linguistics side, studies claim that there are various neural connections between emotional and non-emotional words, where emotionally strong words activate brain regions more strongly due to certain connections with affect reactions, etc. These patterns depend both on the level of language proficiency and on the usual manifestations of emotions, which leads to the fact that the development of emotional vocabulary is the result of experience and cognitive processes. [10]

### ***Memory, Emotion, and Language***

As for the interaction of emotions and memory, studies have concluded that the effect of emotional valence on memory performance differs in the two languages. Researchers claim to improve the memorization of an event or information in general due to a special encoding mechanism in memory, the same effect is absent in another language with the same words of emotions. [10] These differences once again confirm the relationship between emotional expressions, languages, and cognitive processes.

Research on bilingual autobiographical memory shows that emotionally significant experiences are often associated more vividly in the language that was dominant or contextually relevant at the time of encoding [10]. This suggests that language functions as part of the memory that leaves marks on itself rather than as a neutral instrument for later description. As a result, emotional expression tends to be more natural and emotionally rich when produced in the language associated with the first or more salient experience.

Experimental studies further demonstrate that emotional valence has an influence on memory performance differently across languages. Emotional words and phrases are generally recalled more accurately and processed more deeply in the emotionally dominant language, while equivalent expressions in a less dominant language may evoke weaker emotional responses [7]. These findings indicate that emotional vocabulary is not equally grounded across a bilingual's languages.

Thus, differences in memory processing are also reflected in the reaction time and cognitive effort of the bilinguals' emotional expressions. Studies indicate faster recognition,

reaction and processing of emotionally strong words in the dominant language, suggesting stronger associative links between emotion and lexical representation of it[9]. Over time, repeated emotional experiences in one language strengthen these links, reinforcing its emotional salience.

Collectively, cognitive and psycholinguistic research on emotions and bilinguals allows us to identify a complex mechanism of emotional manifestations in bilinguals, including both experience and structural components that form emotionality. [7]

### **Sociocultural and Communicative Contexts**

#### ***Cultural Norms and Emotional Display Rules***

The expression of emotions and norms in cultural and sociocultural contexts are rooted in different ways. These norms of emotional expression place restrictions on the permissibility of expressing certain emotions, degrees of expression, and social contexts. In the case of bilinguals who have two cultural environments from languages, such norms of permissibility also vary from the communicative context and not only from the language. [8]

Just as cultures differ, the languages of these cultures carry different emotional connotations, the distance of social roles, or indicators of prestige and respect. [3] Bilinguals strategically use two languages, depending on their desire to match the social environment, point out boundaries, or express certain emotional signals. An example of such a manifestation may be when bilinguals use one language in an intimate context to express deep feelings to loved ones, while another language is used in formal and more restrained contexts. [1]

#### ***Code Switching as Emotional Strategy***

In more modern scientific research, attention has also been drawn to the role of code switching, that is, language switching in communication as a tool for more accurate expression of emotions in speech. [3] Code switching is not just a linguistic feature, but a whole process of pragmatic processes, which makes speech more detailed in nuances like humor, emotional outbursts or intimacy. [8]

In particular, studies in multilingual contexts often claim that bilinguals often use code switching in particularly emotional moments of interaction in order to more accurately convey feelings or thoughts that are difficult to convey in a second language. [1] This phenomenon in bilingual speech reflects the strategic flexibility of bilingual speech in society and the manifestation of identity.

Delving into the vocabulary of bilinguals, it turns out that some emotional expressions cannot be accurately translated into other languages, that is, there are no equivalents, which encourages you to choose a language in which you can more accurately convey your emotions.

[4] This observation indicates a close relationship between the accessibility of vocabulary and the expression of emotions.

**Conclusion.** Research on the expression of emotions in a bilingual context shows that the use of a particular language in different emotional expressions cannot be limited by the division into the first and second languages. The expression of emotions of bilinguals consists of a combination of different factors such as the dominance of language, accessibility and accuracy of vocabulary, socio-cultural nuances, strategic communication and identity. The peculiarity and authenticity of the expression of emotions should not be fixed by the properties of languages, as this is a reflection of various influences in the form of cognition, culture and context.

Thus, summarizing the results of research on the expression of emotions in bilingualism, it is shown that the expressiveness of emotions and the comfort of communication are frequently

changing phenomena that can be determined more precisely only by personal preferences, environment and a certain situation.

### References:

1. Pavlenko A. Emotions and multilingualism. Cambridge : Cambridge University Press, 2005. – xvi, 306 p.
2. Pavlenko A. Bilingual Selves // Bilingual Minds: Emotional Experience, Expression, and Representation. Bristol, UK : Multilingual Matters, 2006. – pp. 1–33
3. Dewaele J.–M. Emotions in multiple languages. Basingstoke : Palgrave Macmillan, 2010. – xvi, 260 p.
4. Caldwell-Harris C. L. Emotionality differences between languages // Emotion Review. 2014.
5. Marian V., Kaushanskaya M. Words, feelings, and bilingualism: Cross-linguistic differences in emotionality of autobiographical memories // The Mental Lexicon. 2008. Vol. 3, no. 1. – pp. 72–91
6. Harris C. L., Gleason J. B., Ayçiçeği A. When is a first language more emotional? Psychophysiological evidence from bilingual speakers // Bilingual Minds: Emotional Experience, Expression, and Representation. Clevedon, UK : Multilingual Matters, 2006. – pp. 257–284
7. Caldwell-Harris C. L., Ayçiçeği-Dinn A. Emotion-memory in bilinguals: A levels-of-processing approach // Bilingualism: Language and Cognition. 2009. Vol. 12, no. 3. – pp. 291–303
8. Dewaele J.–M., Nakano S. Multilinguals' perceptions of feeling different when switching languages // Journal of Multilingual and Multicultural Development. 2013. Vol. 34, no. 2.
9. Altarriba J. Does cariño equal “liking”? // International Journal of Bilingualism. 2003. Vol. 7, no. 3. – pp. 305–322
10. Schrauf R. W., Rubin D. C. Internal languages of retrieval // Applied Psycholinguistics. 2000. Vol. 21, no. 4. – pp. 445–462

UDC 37.018.43:004.8

**Mamataeva Ramina Adilgazyevna**

Student,  
Program in Information Systems  
I. Zhansugurov Zhetysu University  
(Taldykorgan, Kazakhstan)

**Sakibayev Spartak Razakhovich**

Doctor of Philosophy (PhD), Lecturer  
I. Zhansugurov Zhetysu University  
(Taldykorgan, Kazakhstan)

## ARTIFICIAL INTELLIGENCE IN EDUCATION

**Abstract:** The article examines the integration of artificial intelligence into the educational process through the TPACK framework. The study analyzes how AI tools, specifically chatbots and machine learning, assist educators in combining technological, pedagogical, and content knowledge. Based on a survey of 15 instructors, the research demonstrates the positive impact of AI on the educational landscape while also identifying potential drawbacks, such as a decrease in students' independent thinking.

**Keywords:** artificial intelligence, educational technology, TPACK framework, chatbots, ICT in education, pedagogical knowledge.

**Introduction.** The field of educational technology, also known as edutech, represents a learning approach emphasizing the wide and extensive level of integration between information technologies and educational process. The main goal of this field is replacement of the traditional paper-based teaching media with their digital-based alternatives. Educational technology has achieved a high level of popularity and adoption in the learning process of various subjects taught at secondary and higher education level. In the majority of cases, one of the most adopted ways to integrate educational technology with the learning process is the display of multimedia content with interactive educational content. [1] Also Internet access has always been the main requirement for the usage of ICT in the educational context. [2]

However, the recent trends in the progress and evolvement of modern ICT have caused a tremendous level of changes in the current state of educational technology. The emergence of the theory and practice of AI is expected to have a major influence impact on ICT landscape in general and educational technology in particular. [3][4]

The need for adopting the concepts and methods from AI to educational technology has been accentuated by the studies carried out by researchers and educators from different sectors of education. The published works demonstrate the positive outcomes that the integration of AI and educational technology can bring to the educational process. The existing research covers a multitude of educational advantages that are to be brought both for teachers and students. Thus, as indicated by the research [5][6], the integration of AI and educational technology can

potentially yield academic benefits, encompassing enhancements in students' cognitive abilities and their attitudes toward learning. The findings from [7][8][9][10] also confirm the positive effect that AI can bring to educational technology.

The current study explores how the integration of AI and educational technology can positively affect such area of educational technology as Technological, Pedagogical and Content Knowledge (TPACK) framework. The main emphasis is made on analyzing how the students' attitude towards learning is affected by the adoption of methods from AI.

**Theoretical Framework.** The current study interprets the term “Artificial Intelligence” as software solutions simulating in an efficient way human-like intelligent reasoning and behavior which can bring educational value to learning process.

The Technological Pedagogical and Content Knowledge (TPACK) is defined as a framework within educational technology designed to deal with various challenges that educators and students meet in the process of adoption of ICT tools for the academic purposes. The framework is to provide educators with scientific-based means to overcome various obstacles met in the classroom based on usage of ICT. The TPACK framework serves its intended purpose by finding the most appropriate ways to combine such components as technology, pedagogy, and knowledge [6]. The TPACK framework is based on substantiated assumption the interconnection between technology, the knowledge and the content create conditions for pedagogical advances and is able to facilitate students' academic performance. According to [6] the TPACK framework stresses out three fundamental domains of knowledge. These domains include such components as technological knowledge, pedagogical knowledge, and content knowledge.

The domain of technological knowledge encompasses various ways in which teachers employ ICT tools in their work. It encompasses software and hardware solutions used in the learning process. The main prerequisite of this domain is skills in using various forms of educational technology to increase the effectiveness of the learning process in a classroom. Technological knowledge also requires an ability to keep aligned with the latest technological trends and developments.

The domain of content knowledge deals with the level of knowledge that instructors must possess, related to the academic discipline taught in a classroom. In addition to level of knowledge, this domain also encompasses such auxiliary concepts as learning methodologies and frameworks applied to distribute the knowledge to students. The interpretation of content knowledge differs from one educator to another depending on the specific academic interests and learning environments.

The domain of Pedagogical knowledge included the various ways by which a teacher presents the material and what he does to make this presentation accessible to students. It mostly encompasses methodologies and standard practices used in learning. It also deals with such variables of the learning process as the goals and objectives of learning, lesson planning and scheduling, classroom management etc.

In many instances, instructors opt for a blend of specific domains. The three most prevalent combinations include technological pedagogical knowledge, technological content knowledge, and pedagogical content knowledge.

Technological pedagogical knowledge emerges from the fusion of technical expertise and pedagogical understanding. It encompasses the various interactions established between ICT tools and pedagogical methodologies and concepts.

Pedagogical content knowledge arises from the amalgamation of pedagogical expertise and content knowledge.

It covers interactions and relationships existing between learning goals and pedagogical principles and methodologies.

The domain of technological content knowledge emerges as the result of combination of technological knowledge and content knowledge. It encompasses the relationships that are formed between learning goals and ICT tools used to achieve these goals.

Figure 1 provides a visual presentation of the structure of the TPACK framework.

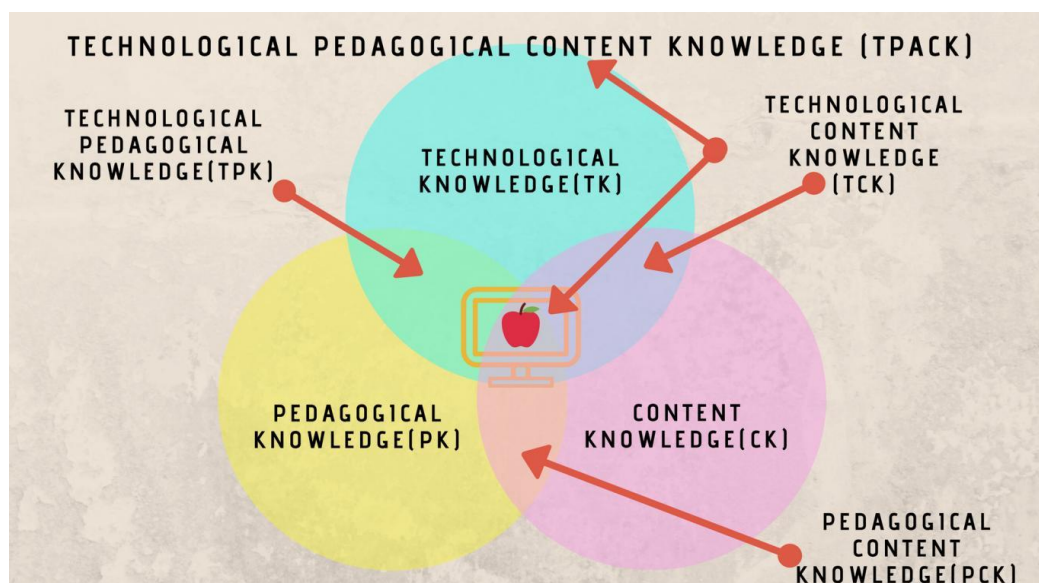


Fig. 1. The structure of the TPACK framework

Using one of these three combinations, it becomes possible for an instructor to use the TPACK framework as the model for increasing the academic outcomes with the means of effective integration of educational technology and the existing learning process. However, the main challenge in this process lies in selecting the most appropriate combination of the described knowledge domains. And to a larger extent, this process can be significantly improved by making use of AI combined with appropriate treatment various factor emerging during the academic activities.

**Methods.** To verify the hypothesis stating the effectiveness of using AI methods in tandem with the TPACK framework an experiment was conducted. The experiment was carried out online and organized by conducting survey and questionnaire among 15 mathematics instructors who use the TPACK framework for training students participating in online Olympiads. Seven of the surveyed instructors specialized in Computer Science, five specialized in mathematics and three in computational physics. The choice of the respondents was made on a random basis to avoid various biases which may affect the evaluation of the survey's results.

The main purpose of the survey was to evaluate the percentage of the respondents which answered a particular question. If a respondent failed to answer a question in one way or another it was considered to be equal to 0 percent. The respondents were given two weeks to complete all the questions and send them back to interviewers.

The questionnaire was distributed to students through the means of email. It contained the following questions given in Table 1:

**Table 1- The items of the questionnaire**

| No | Content                                                                                                                                                                                       |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Do you use the methods provided by Artificial Intelligence in the process of choosing the most appropriate combination of TPACK's knowledge domains for organizing your own teaching process? |
| 2  | Does Artificial Intelligence provide an effective contribution to the improved application of TPACK framework's concepts in a classroom?                                                      |
| 3  | Do you recommend the application of AI methods to students whose classroom uses the concepts of the TPACK framework?                                                                          |
| 4  | Has the usage Artificial Intelligence's concepts in teaching process changed the educational landscape significantly?                                                                         |
| 5  | What specific Artificial Intelligence technology or solution do you use the most for educational purposes?                                                                                    |
| 6  | What are the main drawbacks of using the methods and concepts of Artificial Intelligence in the learning context?                                                                             |

The first, second, third and fifth questions of the questionnaire attracted the responses from all 15 respondents. The fourth question was answered only by 12 respondents, while the last question received the answers from 13 respondents.

The results extracted from the survey were analyzed by the means of online statistical analysis resources. The verification of the obtained data was held by the means of Mann-Whitney U test whose formula is given on the Figure 2 below.

**Formula:**

$$U_x = N_x \cdot N_y + \frac{N_x(N_x + 1)}{2} - \sum r_x$$

Where,  $U_x$  is the Mann Whitney calculation for sample X

$N$  is number in the samples

$\sum r_x$  is the sum of ranks for sample X.

**Fig. 2. The formula for Mann-Whitney Test**

**Results.** Figure 3 below demonstrates the respondents' answers to the first question.

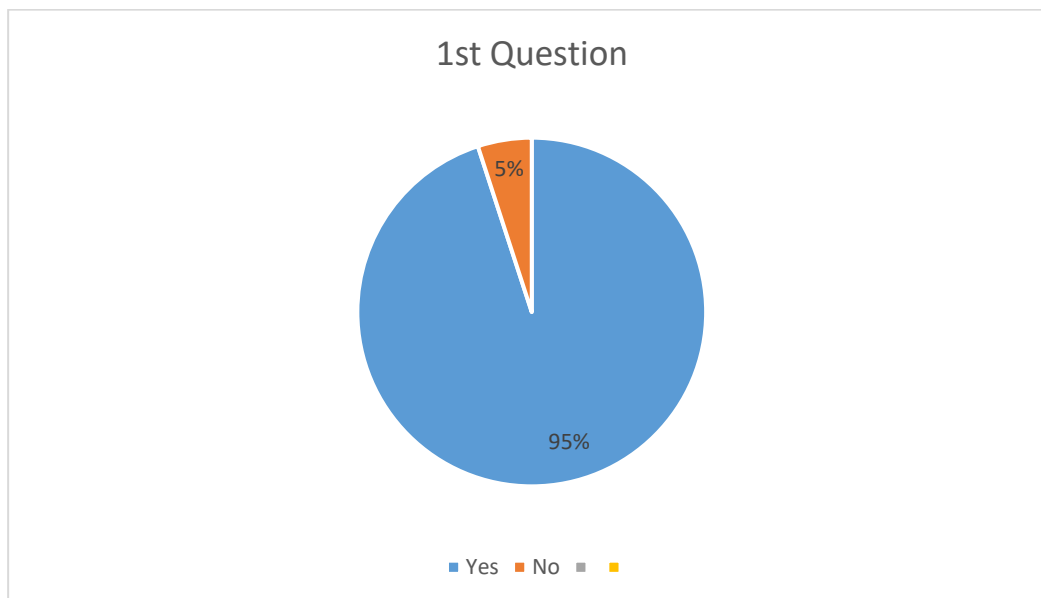


Fig. 3. The answers to the first question

Figure 3 demonstrates that in the majority of cases, the respondents used AI to choose a combination of TPACK's knowledge domains.

Figure 4 below demonstrates the respondents' answers to the second question.

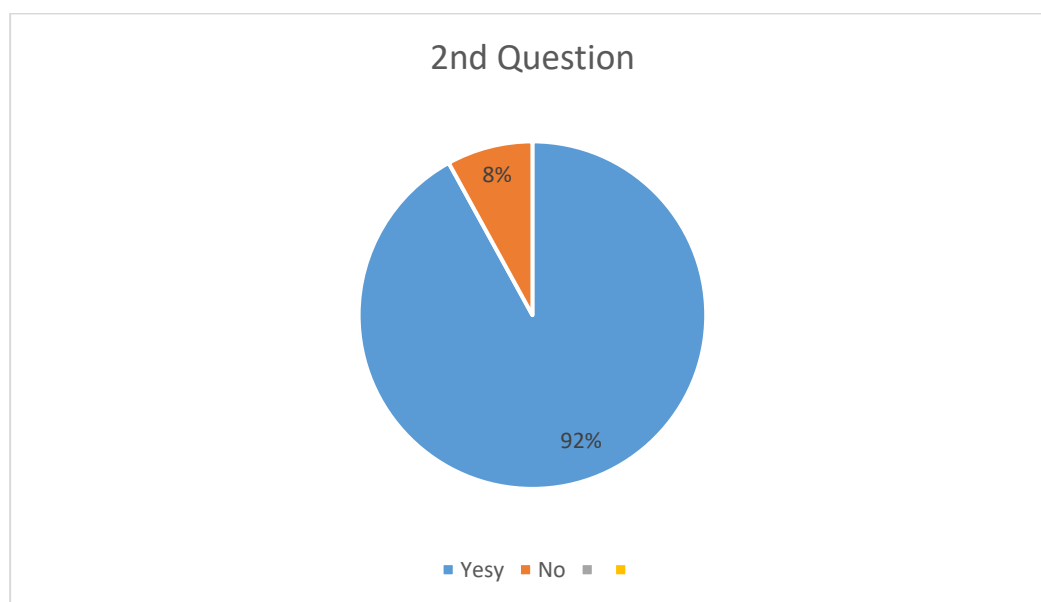


Fig. 4. The answers to the second question

Figure 4 shows that the larger part of the respondents consider AI to be an effective tool for facilitating the usage of TPACK in educational context.

Figure 5 below demonstrates the respondents' answers to the third question.

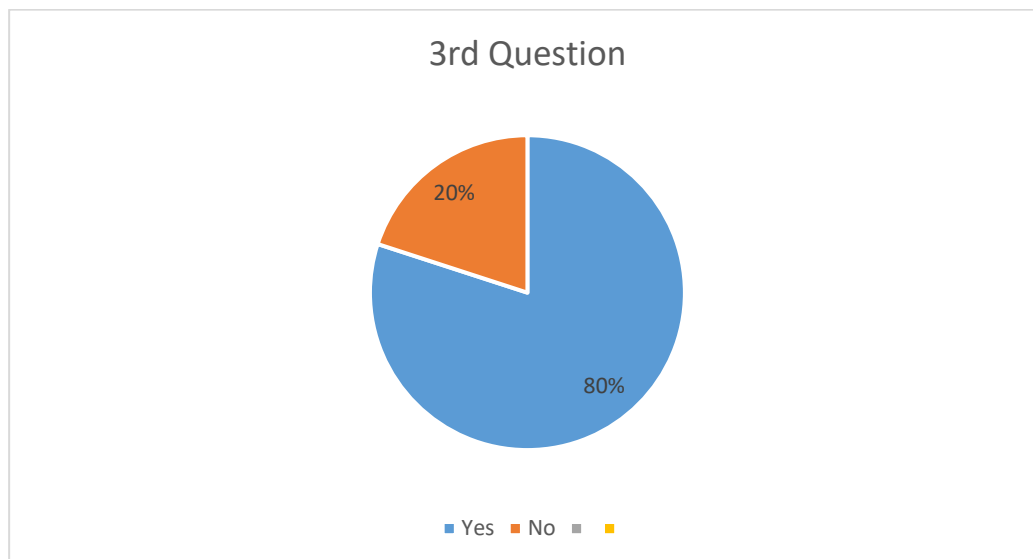


Fig. 5. The answers to the second question

From Figure 5 it is easy to see that the majority of the interviewed recommend the usage of AI to students.

Figure 6 below demonstrates the respondents' answers to the fourth question.

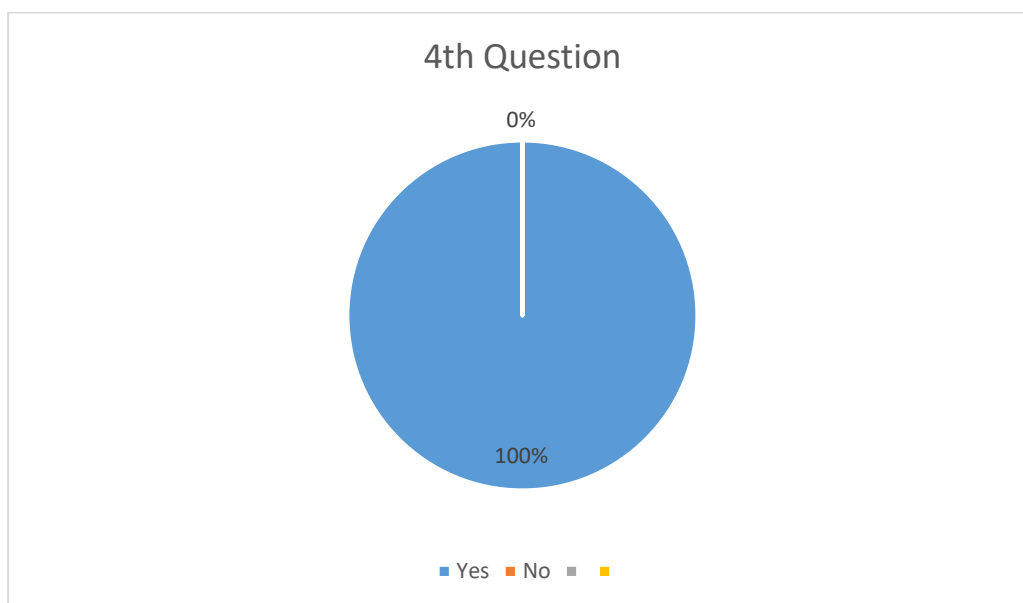


Fig. 6. The answers to the fourth question

Figure 6 demonstrates that all of the respondents consider the learning landscape to be affected considerably by AI.

Table 2 holds the results of the answers to the fifth question of the questionnaire

**Table 2- Results of the answers to the fifth question**

| <i>Answer</i>           | <i>Percentage</i> |
|-------------------------|-------------------|
| <i>Chatbot</i>          | <i>60%</i>        |
| <i>Machine Learning</i> | <i>30%</i>        |
| <i>Deep Learning</i>    | <i>10%</i>        |

As is seen from Table 2 the majority of respondents use chatbots as their main AI technology.

Answering the last item of the questionnaire, 100 percent of the respondents mentioned that the main drawback of using AI is that it has a tendency of reducing students' ability to independent thinking.

**Discussion.** The obtained results demonstrate that the application of AI methods has a major role in the development of ICT in the context of educational technology. The emergence of this concept has significantly changed the current landscape and trends in educational technology. The current survey allows to come to the following conclusion covered below.

Teachers actively use the methods provided by Artificial Intelligence in the process of choosing the most appropriate combination of TPACK's knowledge domains for organizing their own teaching process. This choice is not done randomly, but is based on evaluating the various factors and variables.

Artificial Intelligence does an effective contribution to the improved application of TPACK framework's concepts in a classroom. Moreover, this contribution does not depend on the particular academic discipline.

Teachers actively recommend the usage of AI methods in their learning process, particularly in the field of self-education.

The application of AI practices and concepts in teaching process significantly change the educational landscape and pedagogical approaches.

As the survey shows chatbots are the dominant AI technology used by educators and students.

The results of the current study prove the educational advantages that can be brought by the integration of AI and educational.

**Conclusion.** To increase its effectiveness, educational technology needs to adopt the concepts and methods provided by AI. The need for application of the concepts and methods from AI to educational technology has been accentuated by the studies carried out by researchers and educators from different sectors of education. The published research demonstrates the positive outcomes that the integration of AI and educational technology can bring to the educational process. The existing studies cover a multitude of educational advantages that are to be brought both for teachers and students. Thus, the integration of AI and educational technology can potentially bring many academic benefits, encompassing enhancements in students' cognitive abilities and their attitudes toward learning. The findings from various studies also confirm the positive effect that AI can bring to educational technology.

The current study demonstrates one of the possible ways by which the integration of AI and technology can have a positive impact on the TPACK framework. The main emphasis is made on analyzing how the students' attitude towards learning is affected by the adoption of methods from AI.

### References:

1. Kuimova M. V., Kiyanitsyna A., Truntyagin A. E-learning as a means to improve the quality of higher education learning to undergraduate midwifery students from a practice-based perspective. //Nurse Education in Practice. -2016.- Vol.14(2).
2. Domingo Marta Gómez and Antoni Badia Garganté. Exploring the use of educational technology in primary education: Teachers' perception of mobile technology learning impacts and applications' use in the classroom. //Comput. Hum. Behav. - 2016.-Vol.56-P. 21-28.

3. Al-Takhynéh B. Attitudes towards using mobile applications in teaching mathematics in open learning systems. *International Journal of E-Learning & //Distance Education*. -2018.-Vol. 33(1). -P.1-16.

4. Seo, K., Tang, J., Roll, I. et al. The impact of artificial intelligence on learner–instructor interaction in online learning. *Int J Educ Technol High Educ* **18**, 54 (2021). <https://doi.org/10.1186/s41239-021-00292-9>

5. Seo, K., Fels, S., Yoon, D., Roll, I., Dodson, S., & Fong, M. (2020b). Artificial intelligence for video-based learning at scale. In *Proceedings of the Seventh ACM Conference on Learning@ Scale* (pp. 215–217).

6. Touretzky, D., Gardner-McCune, C., Martin, F., & Seehorn, D. (2019). Envisioning AI for K-12: What should every child know about AI?. In: *Proceedings of the AAAI conference on artificial intelligence* (Vol. 33, No. 01, pp. 9795–9799).

7. Xu Y, Liu X, Cao X, et al. Artificial intelligence: A powerful paradigm for scientific research. *Innovation (Camb)*. 2021;2(4):100179. Published 2021 Oct 28. doi:10.1016/j.xinn.2021.100179

8. Ahmad, S.F., Han, H., Alam, M.M. et al. Impact of artificial intelligence on human loss in decision making, laziness and safety in education. *Humanit Soc Sci Commun* 10, 311 (2023). <https://doi.org/10.1057/s41599-023-01787-8>

9. Hassani, H.; Silva, E.S.; Unger, S.; TajMazinani, M.; Mac Feely, S. Artificial Intelligence (AI) or Intelligence Augmentation (IA): What Is the Future? *AI* 2020, 1, 143-155. <https://doi.org/10.3390/ai1020008>

10. Seo, K., Tang, J., Roll, I. et al. The impact of artificial intelligence on learner–instructor interaction in online learning. *Int J Educ Technol High Educ* 18, 54 (2021). <https://doi.org/10.1186/s41239-021-00292-9>

Электронный научный журнал «Central Asian Scientific Journal»

Редактор: Байдильдинов Т.Ж.  
Комп.верстка: Хусаинов Е.М.

Электронный научный журнал «Central Asian Scientific Journal»  
-2026-1(29)-Астана-ИП ДОС  
Зарегистрировано и выдано свидетельство  
Министерством Информации и Общественного Развития РК  
№KZ40VPY00067791 от 07.04.2023 г.

*За достоверность публикуемой информации, цитат и  
иных изложений ответственность несет автор*



