IQTISODIY TARAQQIYOT VA TAHLIL ILMIY ELEKTRON JURNAL

UO‘K: 004.8:330.3:004.056

GENERATIVE ARTIFICIAL INTELLIGENCE IN ECONOMIC SECTORS: ASSESSING IMPLEMENTATION EFFICIENCY AND ENSURING TECHNOLOGICAL SECURITY

Abdukaxxorova Durdona
Tashkent State University of Economics
ORCID: 0009-0009-4800-3220
abduqaxxorovadurdona64@gmail.com

Abstract. *This article examines the role of generative artificial intelligence in the digital transformation of economic sectors, with a particular focus on assessing implementation efficiency and ensuring technological security. The study argues that generative AI is becoming a strategic tool for improving productivity, operational speed, decision-making quality, and innovation capacity across manufacturing, finance, logistics, public administration, and other sectors. At the same time, the article emphasizes that the benefits of generative AI are accompanied by serious technological risks, including data leakage, model misuse, privacy violations, unreliable outputs, and cybersecurity vulnerabilities. The research is based on a qualitative comparative analysis of recent open-access academic and institutional sources, including OECD, World Bank, NIST, and sector-specific studies. The findings show that the effectiveness of generative AI should be evaluated through a dual framework that combines economic performance indicators with technological security criteria. The article concludes that sustainable implementation requires not only digital infrastructure and organizational adaptation, but also strong governance mechanisms, human oversight, and continuous risk monitoring.*

Keywords: *generative artificial intelligence, digital transformation, economic sectors, implementation efficiency, productivity, technological security, cybersecurity, risk management, innovation, data protection.*

GENERATIV SUN’IY INTELLEKTNING IQTISODIYOT TARMOQLARIDAGI O‘RNI: JORIY ETISH SAMARADORLIGINI BAHOLASH VA TEXNOLOGIK XAVFSIZLIKNI TA’MINLASH

Abdukaxxorova Durdona
Toshkent davlat iqtisodiyot universiteti

Annotatsiya. *Mazkur maqolada iqtisodiyot tarmoqlarining raqamli transformatsiyasi jarayonida generativ sun’iy intellektning o‘rni, xususan, uni joriy etish samaradorligini baholash hamda texnologik xavfsizlikni ta’minlash masalalari tahlil qilingan. Tadqiqotda generativ sun’iy intellekt ishlab chiqarish, moliya, logistika, davlat boshqaruvi va boshqa tarmoqlarda mehnat unumdorligini oshirish, operatsion tezlikni jadallashtirish, qaror qabul qilish sifatini yaxshilash hamda innovatsion salohiyatni kuchaytirishda strategik vosita sifatida namoyon bo‘layotgani asoslab berilgan. Shu bilan birga, uning afzalliklari bilan bir qatorda ma’lumotlar sizib chiqishi, modeldan noto‘g‘ri foydalanish, shaxsiy daxlsizlik buzilishi, ishonchsiz natijalar va kiberxavfsizlikka oid zaifliklar kabi jiddiy texnologik xatarlar ham mavjudligi ta’kidlangan. Tadqiqot OECD, Jahon banki, NIST hamda tarmoqqa oid ochiq manbali ilmiy va institutsional adabiyotlarning sifatli qiyosiy tahliliga asoslangan.*

Natijalar generativ sun'iy intellekt samaradorligini iqtisodiy ko'rsatkichlar va texnologik xavfsizlik mezonlarini birlashtirgan ikki tomonlama yondashuv asosida baholash zarurligini ko'rsatadi. Xulosa sifatida, ushbu texnologiyani barqaror joriy etish uchun nafaqat raqamli infratuzilma va tashkiliy moslashuv, balki kuchli boshqaruv mexanizmlari, inson nazorati hamda uzluksiz risk monitoringi talab etilishi qayd etilgan.

Kalit so'zlar: *generativ sun'iy intellekt, raqamli transformatsiya, iqtisodiyot tarmoqlari, joriy etish samaradorligi, mehnat unumdorligi, texnologik xavfsizlik, kiberxavfsizlik, risklarni boshqarish, innovatsiya, ma'lumotlarni himoya qilish.*

РОЛЬ ГЕНЕРАТИВНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОТРАСЛЯХ ЭКОНОМИКИ: ОЦЕНКА ЭФФЕКТИВНОСТИ ВНЕДРЕНИЯ И ОБЕСПЕЧЕНИЕ ТЕХНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

Абдукаххорова Дурдона
Ташкентский государственный экономический университет

Аннотация. *В данной статье рассматривается роль генеративного искусственного интеллекта в процессе цифровой трансформации отраслей экономики, с особым акцентом на оценку эффективности его внедрения и обеспечение технологической безопасности. В исследовании обосновано, что генеративный искусственный интеллект становится стратегическим инструментом повышения производительности труда, ускорения операционных процессов, улучшения качества принятия решений и усиления инновационного потенциала в промышленности, финансах, логистике, государственном управлении и других секторах. Вместе с тем подчеркивается, что наряду с преимуществами использование данной технологии сопровождается серьезными технологическими рисками, включая утечку данных, неправомерное использование моделей, нарушение конфиденциальности, недостоверность результатов и уязвимости в сфере кибербезопасности. Исследование основано на качественном сравнительном анализе современных открытых академических и институциональных источников, включая материалы OECD, Всемирного банка, NIST, а также отраслевые исследования. Полученные результаты показывают, что эффективность генеративного искусственного интеллекта должна оцениваться на основе двойной модели, объединяющей показатели экономической эффективности и критерии технологической безопасности. В заключении отмечается, что устойчивое внедрение требует не только развитой цифровой инфраструктуры и организационной адаптации, но и эффективных механизмов управления, человеческого контроля и постоянного мониторинга рисков.*

Ключевые слова: *генеративный искусственный интеллект, цифровая трансформация, отрасли экономики, эффективность внедрения, производительность, технологическая безопасность, кибербезопасность, управление рисками, инновации, защита данных.*

Introduction.

Generative artificial intelligence has rapidly become one of the most influential digital technologies shaping modern economic transformation. Unlike earlier automation tools that mainly replaced routine labor, generative AI can support analytical, creative, communicative, and decision-making tasks across manufacturing, finance, logistics, public administration, education, and service industries. Recent OECD research shows that AI, including generative AI, has the potential to affect productivity, innovation, entrepreneurship, and business operations at a system-wide level, making it a general-purpose technology with broad macroeconomic significance]. At the same time, its diffusion is uneven, and its benefits depend on

complementary investments in data infrastructure, human capital, organizational redesign, and governance mechanisms (Calvino, va boshq., 2025).

The growing relevance of generative AI for economic sectors is linked not only to its ability to automate tasks, but also to its capacity to augment workers' skills, accelerate information processing, improve forecasting, reduce search costs, and support faster managerial responses. OECD evidence indicates that generative AI can improve productivity, lower entry barriers for firms, stimulate innovation, and enhance entrepreneurial experimentation, especially in knowledge-intensive and digitally mature environments (Calvino et al., 2025). In addition, broader AI studies suggest that productivity effects are strongest when firms combine technological adoption with process innovation and institutional adaptation (Filippucci et al., 2024). This means that the success of generative AI implementation should not be measured only by technical deployment, but by its real contribution to efficiency, operational quality, and value creation.

However, the rapid spread of generative AI also creates significant economic and technological risks. The World Bank warns that developing and emerging economies may face "premature de-professionalization" if they adopt generative AI without building domestic capabilities, skills, and strategic sectoral integration (Liu., 2024). In other words, generative AI may widen productivity gaps rather than reduce them if adoption occurs in a fragmented, unsafe, or institutionally weak environment. Therefore, questions of implementation efficiency must be assessed together with technological security, data protection, model reliability, and organizational resilience.

This article examines how generative AI can be implemented effectively in economic sectors and how its efficiency may be evaluated while ensuring technological security. The paper argues that the real value of generative AI lies not in the mere use of advanced models, but in building a secure and measurable ecosystem in which productivity gains, innovation outcomes, and risk controls are aligned (Liu., 2024).

Literature review.

The recent literature on generative AI emphasizes three closely connected dimensions: productivity and efficiency gains, sector-specific operational transformation, and the security risks associated with model deployment. OECD research reviewing experimental studies finds that generative AI can improve productivity, innovation, and entrepreneurship by automating repetitive cognitive tasks, enhancing worker performance, and accelerating idea generation and business experimentation (Calvino va boshq., 2025). Earlier OECD work also explains that AI's economic impact emerges through multiple channels, including process optimization, knowledge diffusion, innovation spillovers, and complementarities with digital infrastructure and managerial practices (Filippucci et al., 2024). These findings suggest that generative AI should be studied not as an isolated software tool, but as part of broader digital transformation.

A second body of literature explores sectoral implementation. In manufacturing, firm-level evidence from China shows that greater generative AI adoption intensity is associated with stronger operational capability and improved sustainable performance, indicating that AI can contribute to more efficient production management, resource allocation, and adaptive decision-making (He, 2025). This supports the view that generative AI may produce measurable economic gains when embedded into concrete workflows rather than used only experimentally. Sectoral evidence from cybersecurity operations also shows practical efficiency benefits. A study based on live security operations center data reports that generative AI adoption was associated with a 30.13% reduction in mean time to resolution for security incidents, suggesting that AI can improve speed and responsiveness in high-pressure operational environments (Bono, Grana and Xu, 2024).

A third strand of the literature highlights risks. The World Bank notes that generative AI may reshape comparative advantage, labor demand, and professional services, creating both

growth opportunities and structural vulnerabilities, especially where institutional preparedness is limited (Liu, 2024). From a risk-governance perspective, NIST's Generative AI Profile stresses that organizations must manage risks related to accuracy, privacy, security, transparency, harmful content, and downstream misuse through structured governance, measurement, and continuous monitoring (National Institute of Standards and Technology (NIST, 2024). OWASP similarly identifies key security threats in large language model applications, including prompt injection, sensitive information disclosure, supply-chain vulnerabilities, data and model poisoning, improper output handling, and excessive agency (OWASP Foundation, 2025). Together, these studies show that efficiency and security are not separate concerns; they are interdependent conditions of sustainable AI adoption.

Overall, the literature indicates that generative AI can improve productivity and operational performance, but its sectoral benefits are conditional on governance quality, human oversight, and security architecture. This gap between technical promise and institutional readiness makes it necessary to develop an integrated framework for evaluating efficiency and ensuring technological safety in economic sectors (OWASP Foundation, 2025).

Research methodology.

This study uses a qualitative analytical methodology based on comparative literature synthesis and conceptual framework development. The analysis relies on recent open-access sources from OECD, the World Bank, NIST, OWASP, and peer-reviewed or research-based sectoral studies on manufacturing and cybersecurity operations (OWASP Foundation, 2025). These materials were selected because they collectively cover the three core dimensions of the research problem: economic efficiency, sectoral implementation, and technological security.

The methodological approach consists of four stages. First, the study identifies the main channels through which generative AI influences efficiency in economic sectors, including labor augmentation, faster information processing, operational optimization, reduced response time, and innovation support (Bono, Grana and Xu, 2024). Second, it compares how these effects appear across different sectors, especially in production management and security operations, in order to distinguish direct process effects from broader organizational effects (He, 2025). Third, the study reviews major technological security risks associated with generative AI systems, including privacy breaches, model misuse, unsafe integrations, poisoning, prompt injection, and insecure outputs. For the purposes of this article, implementation efficiency is interpreted through five analytical indicators: productivity growth, quality improvement, time reduction, decision support performance, and innovation capacity. Technological security is interpreted through five corresponding safeguards: data confidentiality, model integrity, access control, output reliability, and continuous risk monitoring .This paired approach is important because a generative AI system cannot be considered efficient in economic terms if it simultaneously introduces unacceptable security, privacy, or operational risks.

Analysis and discussion of results.

The analysis shows that generative AI can increase efficiency in economic sectors through both direct and indirect mechanisms. Directly, it reduces the time required for routine cognitive tasks such as drafting, summarizing, classification, reporting, customer interaction, code assistance, and incident analysis (Calvino, Reijerink and Samek, 2025; Bono, Grana and Xu, 2024). Indirectly, it strengthens organizational learning, supports experimentation, and improves coordination across departments and processes (Calvino, Reijerink and Samek, 2025; Filippucci et al., 2024). This means that the economic effect of generative AI is not limited to labor substitution; it also includes labor augmentation and workflow redesign.

The sectoral evidence reinforces this conclusion. In manufacturing, generative AI contributes to stronger production management capability and better sustainable performance when firms integrate it into operations rather than treat it as a peripheral digital tool (He,

2025). In security operations, measurable gains appear in the form of faster incident resolution, showing that generative AI can improve response efficiency in environments where time and decision quality are critical (Bono, Grana and Xu, 2024). These findings suggest that the best results occur when AI is embedded into specific business functions with clear performance metrics.

At the same time, the study finds that efficiency gains are highly fragile if technological security is weak. NIST emphasizes that generative AI systems create risks linked to trustworthiness, privacy, explainability, harmful outputs, and misuse across the full lifecycle of design, deployment, and monitoring (National Institute of Standards and Technology (NIST), 2024). OWASP's security framework for LLM applications further demonstrates that AI systems are vulnerable not only at the model level, but also through interfaces, connected tools, datasets, orchestration pipelines, and user interactions (OWASP Foundation, 2025). Therefore, organizations that introduce generative AI into economic sectors without adequate safeguards may experience hidden costs, including data leakage, compliance failures, erroneous decisions, reputational damage, and operational disruption.

Based on the reviewed evidence, the article identifies five mechanisms for ensuring secure and effective implementation. First, organizations should define sector-specific performance indicators before deployment, such as cost reduction, turnaround time, output quality, customer satisfaction, or incident response efficiency (Bono, Grana and Xu, 2024). Second, they should implement governance procedures for data handling, access rights, human review, and auditability in line with trustworthy AI principles (National Institute of Standards and Technology (NIST), 2024). Third, AI systems must be protected against prompt injection, sensitive information disclosure, poisoning, and insecure integrations through technical controls and security testing (OWASP Foundation, 2025). Fourth, adoption strategies should include workforce training, because productivity benefits are amplified when workers know how to use AI critically and responsibly. Fifth, implementation should proceed iteratively, with pilot testing, performance review, and risk reassessment before large-scale diffusion (National Institute of Standards and Technology (NIST), 2024).

Table 1.

Comparative analysis of Generative AI implementation across economic sectors

Economic sector	Main application of Generative AI	Expected efficiency gains	Main technological security risks	Evaluation indicators
Manufacturing	Production planning, predictive reporting, process optimization	Higher productivity, lower downtime, better resource allocation	Data leakage, model errors, integration vulnerabilities	Output per worker, production time, defect rate
Banking and finance	Automated customer service, fraud pattern analysis, report generation	Faster service, lower operational costs, improved analytics	Privacy breaches, cyberattacks, biased outputs	Transaction speed, service cost, customer satisfaction
Logistics	Route planning, demand forecasting, document automation	Reduced delivery time, optimized inventory, lower logistics costs	System manipulation, inaccurate forecasting, data exposure	Delivery time, storage cost, forecast accuracy
Healthcare economy	Medical documentation, decision support, service communication	Time saving, improved service management, better coordination	Sensitive data exposure, reliability issues, compliance risks	Service speed, administrative cost, accuracy level
Public administration	Automated reporting, citizen communication, document analysis	Faster service delivery, reduced bureaucracy, better transparency	Confidentiality risks, misinformation, weak access control	Processing time, service quality, citizen satisfaction

As a result, the study proposes a central conclusion: in economic sectors, generative AI efficiency should be evaluated through a dual criterion. The first criterion is economic performance, measured by productivity, quality, speed, and innovation. The second criterion is technological security, measured by confidentiality, integrity, resilience, reliability, and governance maturity. Only the combination of these two dimensions can produce sustainable digital transformation (OWASP Foundation, 2025).

Conclusion and suggestions.

Generative artificial intelligence is becoming a strategic tool for the transformation of economic sectors. The reviewed literature shows that it can improve productivity, strengthen innovation, support operational management, and enhance organizational responsiveness across different fields (Bono, Grana and Xu, 2024). Nevertheless, its positive economic effects are neither automatic nor universal. They depend on institutional capacity, workforce preparedness, process redesign, and the existence of reliable governance and security systems (National Institute of Standards and Technology (NIST, 2024).

This study demonstrates that implementation efficiency and technological security must be treated as a single policy and management agenda. A generative AI solution that improves short-term speed but creates long-term vulnerabilities cannot be considered truly efficient. Likewise, a highly secure system with no measurable contribution to productivity or service quality cannot justify wide-scale adoption. The most effective approach is balanced deployment based on measurable results, human oversight, secure architecture, and continuous monitoring (Bono, Grana and Xu, 2024).

For economic sectors, the practical implication is clear: generative AI should be introduced through staged implementation models, with explicit performance indicators, risk controls, and regular evaluation. Policymakers and enterprise managers should support not only adoption itself, but also sector-specific standards for data governance, cybersecurity, workforce upskilling, and responsible AI use (National Institute of Standards and Technology (NIST), 2024). In this way, generative AI can become not simply a technological trend, but a secure and productive driver of long-term economic modernization.

References /Adabiyotlar/ Литература:

Bono, J., Grana, J. and Xu, A. (2024) Generative AI and security operations center productivity: Evidence from live operations. arXiv.

Calvino, F., Reijerink, J. and Samek, L. (2025) The effects of generative AI on productivity, innovation and entrepreneurship. OECD Artificial Intelligence Papers. OECD Publishing.

Filippucci, F. et al. (2024) The impact of artificial intelligence on productivity, distribution and growth: Key mechanisms, initial evidence and policy challenges. OECD Artificial Intelligence Papers, No. 15. OECD Publishing.

He, M. (2025) How generative AI empowers production management to achieve sustainable performance: Insights from China's manufacturing industry. Frontiers in Artificial Intelligence.

Liu, Y. (2024) Generative AI: Catalyst for growth or harbinger of premature de-professionalization? World Bank Policy Research Working Paper. World Bank.

National Institute of Standards and Technology (NIST) (2024) Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (AI 600-1).

OWASP Foundation (2025) OWASP Top 10 for Large Language Model Applications 2025.