AUDİT 2025, 1 (47), səh. 100-111.
AUDIT 2025, 1 (47), pp. 100-111.
АУДИТ 2025, 1 (47), стр. 100-111.

DOI: **10.59610/bbu1.2025.1.9**

Abdulla Ibrahim Abdullayev,
Ph.D. Student,
Baku Business University,
E-mail: abdullaabdullayev222@gmail.com

UDC: 004.8, 339.138, 330.34, 004
JEL: L81, O33, D80, F52

THE IMPACT OF DIGITALIZATION AND ARTIFICIAL INTELLIGENCE ON ECONOMIC SECURITY IN E-COMMERCE

A B S T R A C T

The purpose of the research – the increasing integration of digitalization and artificial intelligence (AI) in e-commerce has transformed the economic security landscape, presenting both opportunities and challenges. This research explores how AI-driven solutions impact e-commerce by enhancing efficiency, detecting fraud, and improving regulatory compliance. The study examines key risks associated with AI, including data security threats and ethical concerns, while identifying strategies for balancing innovation with security.

The methodology of the research – this study employs a mixed-methods approach, combining qualitative and quantitative analyses to assess AI's role in securing digital trade. A comprehensive review of recent academic literature, industry case studies, and statistical data is conducted to identify emerging trends and best practices. The research further evaluates the effectiveness of AI-driven fraud detection, supply chain security, and privacy-preserving mechanisms in digital commerce.

The practical importance of the research – the findings of this study provide valuable insights for e-commerce businesses, policymakers, and regulatory bodies. By understanding how AI influences economic security, businesses can implement proactive strategies to mitigate risks and enhance trust in digital transactions. Policymakers can use these insights to refine regulatory frameworks, ensuring AI adoption aligns with ethical and security standards.

The originality and scientific novelty of the research – while previous studies have explored AI applications in e-commerce, this research integrates security-focused perspectives to provide a holistic understanding of AI's impact on economic resilience. By bridging technological advancements with security challenges, this study contributes to the ongoing discourse on sustainable AI adoption in digital markets.

Keywords: artificial intelligence, digitalization, economic security, e-commerce, cyber-security, risk management, AI in business, regulatory compliance.

AUDİT 2025, 1 (47), səh. 100-111.
AUDIT 2025, 1 (47), pp. 100-111.
АУДИТ 2025, 1 (47), стр. 100-111.

INTRODUCTION

The rapid evolution of digitalization and artificial intelligence (AI) has revolutionized the global e-commerce sector, enabling unprecedented efficiency and growth. AI-powered algorithms facilitate personalized shopping experiences, automate logistics, and optimize pricing strategies, fundamentally reshaping consumer behavior and business models [1, 47]. However, alongside these benefits, the increasing reliance on AI introduces significant challenges, particularly concerning economic security, cybersecurity vulnerabilities, and regulatory compliance. The widespread integration of AI in e-commerce requires businesses to assess the balance between leveraging AI-driven innovations and managing the risks associated with automation [2, 45].

Economic security in e-commerce is closely tied to the ability of businesses to protect financial transactions, customer data, and digital assets from cyber threats. As AI-driven automation becomes more prevalent, businesses face the dual challenge of leveraging technology for growth while mitigating security risks. The rise of sophisticated cyberattacks, AI-powered fraud mechanisms, and deepfake scams has intensified concerns regarding digital trade resilience [3, 112]. Moreover, cybercriminals are now using AI to enhance the effectiveness of phishing scams and automated hacking techniques, making traditional security measures insufficient in combating these evolving threats [4, 175]. AI-driven fraud detection and risk assessment tools, however, provide effective countermeasures, identifying anomalies in transaction patterns and preventing fraudulent activities in real time [5, 90].

Furthermore, AI's capability to process vast amounts of personal data raises ethical and regulatory concerns, necessitating comprehensive governance frameworks to balance innovation with consumer rights. The European Union's General Data Protection Regulation (GDPR) and similar policies worldwide are setting new compliance standards, requiring businesses to ensure data privacy and security in AI-driven transactions [3, 112]. The challenge lies in the fact that regulatory frameworks often struggle to keep pace with the rapid advancements of AI technologies, leading to legal ambiguities and enforcement gaps [5, 90]. This complexity makes it essential for businesses and policymakers to collaborate on developing adaptive strategies that ensure compliance while fostering innovation.

Beyond security concerns, AI-driven automation in e-commerce also has implications for workforce dynamics and business sustainability. While automation improves efficiency and reduces operational costs, it also raises concerns about job displacement and ethical AI deployment. Ensuring that AI adoption does not exacerbate economic inequalities requires proactive policies and strategic workforce planning [1, 47]. Businesses must invest in AI literacy and workforce reskilling initiatives to create an ecosystem where human expertise complements technological advancements rather than being replaced by them.

This study explores the interplay between digitalization, AI, and economic security in e-commerce. By examining AI-driven fraud detection, cybersecurity strategies, and regulatory measures, this research aims to provide actionable insights into enhancing security within the digital economy. The following analyze the key risks and opportunities associated with AI in e-commerce and propose solutions to ensure a secure and sustainable digital marketplace.

AUDİT 2025, 1 (47), səh. 100-111.
AUDIT 2025, 1 (47), pp. 100-111.
АУДИТ 2025, 1 (47), стр. 100-111.

Discussions and Results

Artificial Intelligence (AI) has significantly transformed the landscape of e-commerce, offering both innovative opportunities and complex challenges. The theoretical foundation of AI in economic security is built upon its capabilities in automation, predictive analytics, and cybersecurity enhancement. AI-driven systems leverage vast amounts of data to optimize decision-making, streamline supply chains, and improve fraud detection mechanisms [6, 47]. Machine learning models enable businesses to detect patterns in customer behavior, forecast market trends, and mitigate financial risks associated with digital transactions [7, 112]. The ability of AI to process and analyze big data in real time has led to improvements in operational efficiency, cost reduction, and risk minimization. These AI-driven applications not only optimize revenue generation but also help companies proactively manage potential security threats in digital transactions.

The theoretical framework of AI in economic security is closely linked to risk management principles. The implementation of AI-driven risk assessment models helps identify vulnerabilities in e-commerce platforms, reducing financial losses due to fraudulent activities. Advanced AI systems can monitor millions of transactions in real-time, flagging anomalies that indicate potential fraud, which would be nearly impossible to detect manually [8, 89]. Moreover, AI plays a critical role in strengthening consumer trust by ensuring secure transactions and protecting sensitive data from cyber threats. With cyberattacks becoming increasingly sophisticated, AI-powered cybersecurity tools are essential in combating digital fraud and reinforcing security infrastructures [9, 102]. AI is being actively used to predict and mitigate cyber threats by leveraging behavioral analysis and anomaly detection techniques, further reducing the risk of data breaches and unauthorized transactions.

Another critical dimension of AI's impact on economic security is its role in regulatory compliance. As digital markets expand, regulatory bodies are implementing stricter policies on data privacy and AI governance to protect consumers from exploitative practices. AI technologies assist businesses in ensuring compliance with evolving regulations by automating audits, tracking data usage, and generating compliance reports [10, 76]. The increasing role of AI in regulatory compliance indicates its potential not just as an operational tool but also as an integral part of legal and ethical business practices. However, there is a growing concern about AI's interpretability and the ethical challenges it poses, such as biased decision-making and privacy infringements. Addressing these concerns requires a balance between AI innovation and human oversight to ensure economic security remains a priority.

From a personal perspective, AI's role in economic security is not just about automation and fraud detection—it is also about enhancing the resilience of businesses in the face of economic uncertainties. The ability of AI to predict financial risks and market fluctuations enables businesses to take proactive measures, ultimately contributing to economic stability. Furthermore, AI-driven risk management models can help small and medium enterprises (SMEs) access better financial planning tools, enabling them to compete with larger corporations. However, as AI systems become more autonomous, there is an increased need for

AUDİT 2025, 1 (47), səh. 100-111.
AUDIT 2025, 1 (47), pp. 100-111.
АУДИТ 2025, 1 (47), стр. 100-111.

ethical governance frameworks that ensure fairness, transparency, and accountability in AI-driven decision-making processes.

The continuous evolution of AI technology calls for adaptive strategies to address emerging security risks while maintaining economic stability in digital markets. As AI continues to redefine the e-commerce landscape, businesses and policymakers must work together to establish ethical and regulatory frameworks that support AI-driven economic security. The integration of AI with traditional risk management practices is essential for building a secure, trustworthy, and resilient digital economy that benefits businesses, consumers, and society as a whole.

Despite its numerous advantages, AI integration in e-commerce comes with significant challenges that threaten economic security. As AI-driven systems become more sophisticated, so do the cyber threats that exploit vulnerabilities within digital marketplaces. One of the most pressing concerns is cybersecurity. AI-powered cyberattacks, including deepfake fraud, AI-enhanced phishing scams, and automated hacking tools, have become more advanced, making traditional security measures insufficient. Cybercriminals are now utilizing AI to develop intelligent malware that can adapt to security defenses, evade detection, and carry out large-scale data breaches. Businesses must develop proactive security measures that incorporate AI-based threat detection systems capable of identifying and neutralizing cyber risks before they escalate [11, 175]. AI-driven security solutions such as biometric authentication, anomaly detection, and behavioral analytics have shown promise in mitigating cyber threats, but they require constant refinement to stay ahead of malicious AI applications. As digital transactions grow in volume, e-commerce businesses cannot rely solely on reactive measures but must integrate predictive AI-driven cybersecurity protocols that anticipate attacks before they occur.

Another critical challenge associated with AI in e-commerce is algorithmic bias and fairness. AI models are trained on large datasets, and if these datasets contain historical biases, the algorithms may reinforce and perpetuate discriminatory outcomes. In e-commerce, biased AI algorithms can result in unfair pricing, discriminatory lending decisions, and exclusionary marketing strategies. For example, some AI-based credit scoring models have been found to disproportionately disadvantage certain demographic groups due to biased training data. The lack of transparency in AI decision-making further exacerbates this issue, as businesses and consumers often have little insight into how AI-driven decisions are made [12, 90]. This challenge not only undermines trust in AI but can also have legal consequences as regulatory bodies increasingly scrutinize AI-driven processes for potential discrimination. Businesses that fail to address algorithmic bias may face reputational damage and financial penalties, making it essential to invest in fairness-aware machine learning and diverse data representation. Additionally, integrating human oversight in AI decision-making processes can provide an additional layer of accountability, ensuring that AI-powered recommendations align with ethical and inclusive practices.

Data privacy is another major challenge that arises with the extensive use of AI in e-commerce. AI-driven platforms collect vast amounts of personal information, including

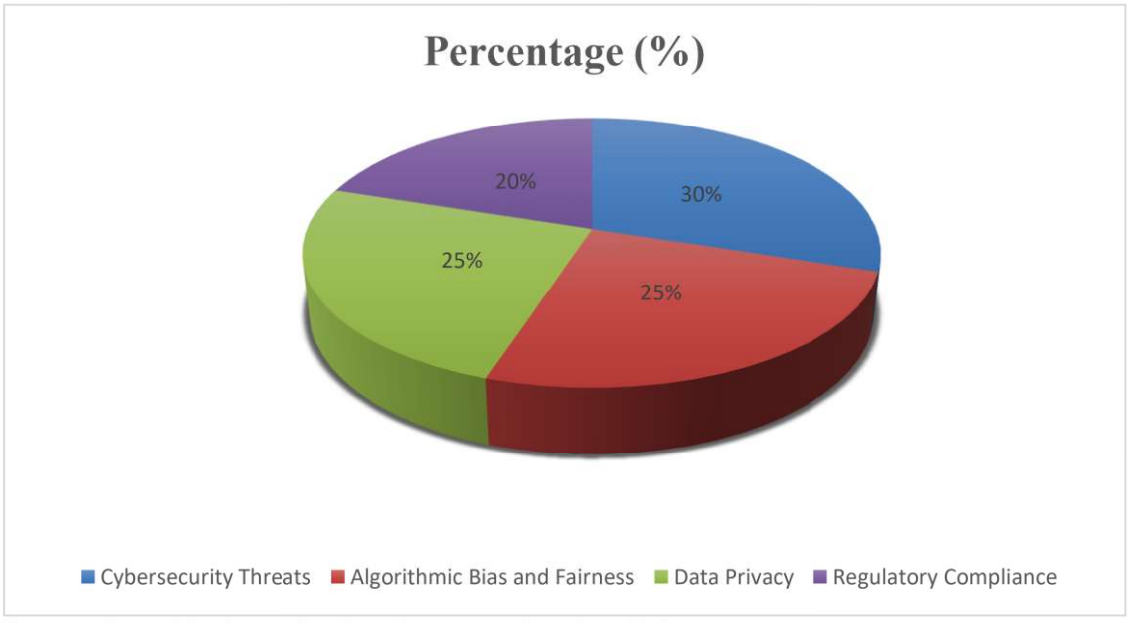
AUDİT 2025, 1 (47), səh. 100-111.
AUDIT 2025, 1 (47), pp. 100-111.
АУДИТ 2025, 1 (47), стр. 100-111.

transaction history, browsing behavior, biometric data, and social interactions. While this data enhances personalization and customer experience, it also raises concerns about how information is stored, shared, and utilized. Unauthorized data access, data leaks, and AI-driven surveillance systems pose serious privacy threats. In many cases, consumers are unaware of the extent to which their data is collected and analyzed, leading to concerns about consent and data ownership. The lack of transparent AI decision-making processes contributes to consumer distrust, making it imperative for businesses to implement robust governance frameworks that ensure ethical AI deployment. Transparency reports, explainable AI models, and user-controlled data settings are essential to building consumer confidence in AI-powered e-commerce platforms [13, 112]. However, beyond transparency, companies must also prioritize data minimization strategies, collecting only the necessary information required for their operations rather than indiscriminately gathering excessive user data. Organizations should also consider decentralized privacy-preserving techniques such as federated learning, which allows AI models to learn from user data without directly accessing or storing it in central servers.

The regulatory landscape surrounding AI is another evolving challenge. The rapid pace of AI advancements often outstrips regulatory efforts, creating gaps in compliance and legal uncertainties that can impact global e-commerce operations. Governments and policymakers struggle to keep up with AI-driven business models, leading to inconsistencies in regulations across different jurisdictions. For instance, while the European Union has implemented strict data protection laws such as the General Data Protection Regulation (GDPR), other regions have more lenient regulatory frameworks, allowing businesses to operate with minimal oversight.

Diagram 1.

Distribution of AI Challenges in E-Commerce



Source: Created by the author based on research and analysis.

AUDİT 2025, 1 (47), səh. 100-111.
AUDIT 2025, 1 (47), pp. 100-111.
АУДИТ 2025, 1 (47), стр. 100-111.

This discrepancy creates compliance challenges for multinational e-commerce companies that must navigate a fragmented regulatory environment [14, 134]. Without clear international standards, companies face difficulties in ensuring that their AI applications adhere to multiple regional legal requirements. To address this challenge, there is an increasing need for AI governance coalitions where regulators, industry leaders, and policymakers collaborate to develop global AI security standards. Rather than adopting isolated regional policies, a unified regulatory approach could provide clearer guidelines on AI data processing, algorithmic accountability, and ethical implementation in digital markets.

The pie chart Diagram 1 titled "Distribution of AI Challenges in E-Commerce" visually represents the key risks associated with AI integration in the digital marketplace, highlighting their relative impact on economic security. Cybersecurity threats (30%) emerge as the most significant challenge, as AI-driven cyberattacks such as deepfake fraud, AI-enhanced phishing scams, and automated hacking tools become increasingly sophisticated. Businesses must develop proactive defense mechanisms to mitigate these evolving threats. Algorithmic bias and fairness (25%) follow closely, as AI models trained on biased datasets can reinforce discrimination in pricing, lending decisions, and personalized marketing, raising ethical and legal concerns. Similarly, data privacy (25%) poses a major risk, as AI-driven platforms collect and process vast amounts of user data, leading to concerns about unauthorized access, surveillance, and consumer consent. Companies must ensure transparency in data handling to maintain trust. Lastly, regulatory compliance (20%) remains a challenge, with AI advancements often outpacing existing legal frameworks, leaving businesses struggling to navigate global compliance requirements.

This distribution highlights the interconnected nature of AI challenges, where security risks, ethical considerations, and regulatory demands must all be addressed simultaneously. While cybersecurity threats take precedence, businesses cannot ignore the pressing need for fairness, privacy protection, and regulatory adherence. As AI continues to evolve, organizations must adopt a balanced approach that fosters innovation while mitigating risks, ensuring that AI-driven e-commerce remains both secure and ethically sound.

From a personal perspective, the integration of AI into e-commerce security frameworks is both an opportunity and a risk. On the one hand, AI enhances fraud detection, strengthens cybersecurity, and optimizes risk management strategies. However, on the other hand, the increasing sophistication of AI-driven threats means that businesses must constantly evolve their defense mechanisms. There is also a significant need for ethical AI frameworks that prioritize fairness, consumer rights, and regulatory compliance without stifling innovation. As AI continues to reshape e-commerce, the focus should be on fostering a balanced approach that leverages AI's strengths while addressing its associated risks. Businesses must take proactive steps to ensure AI is deployed responsibly, transparently, and in a way that upholds economic security without compromising ethical standards. The future of AI in e-commerce will depend on companies' willingness to align their innovation strategies with ethical considerations, ensuring that technology serves the interests of businesses and consumers alike.

AI has introduced a range of applications that significantly enhance economic security in e-commerce by improving fraud detection, optimizing supply chain management, and

AUDİT 2025, 1 (47), səh. 100-111.
AUDIT 2025, 1 (47), pp. 100-111.
АУДИТ 2025, 1 (47), стр. 100-111.

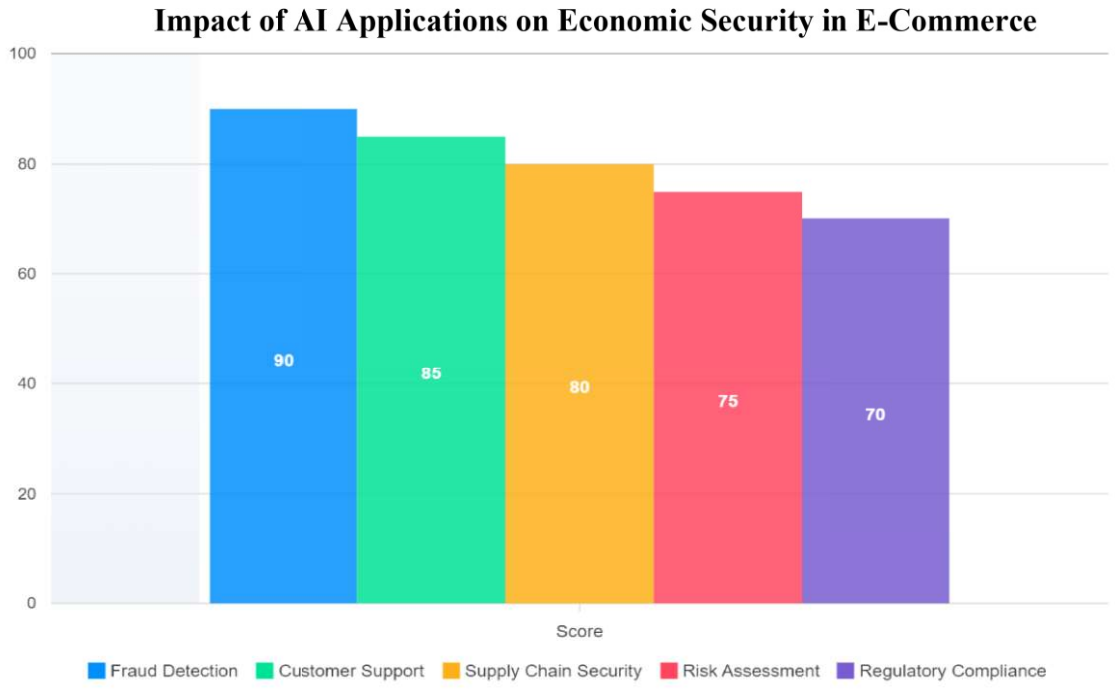
strengthening customer support services. One of the most impactful implementations of AI in digital security is fraud detection. As cyber threats evolve and become more sophisticated, traditional fraud detection methods often struggle to keep up with the sheer volume of transactions and the complexity of modern digital fraud tactics. AI-powered fraud detection systems provide a proactive approach by analyzing transaction patterns, detecting unusual behaviors, and identifying suspicious activities in real time. These systems utilize machine learning models that continuously learn from fraudulent activity, enabling them to adapt and improve detection accuracy over time. This capability significantly reduces financial losses for businesses and minimizes the risk of fraudulent transactions disrupting e-commerce platforms [15, 47]. Additionally, AI enhances fraud prevention by automating identity verification, using biometric authentication, and flagging suspicious login attempts, ensuring that only authorized users can access accounts.

Beyond fraud prevention, AI plays a crucial role in enhancing supply chain security by improving logistics, inventory management, and risk mitigation. The global supply chain is increasingly vulnerable to disruptions caused by cyberattacks, logistical inefficiencies, and unpredictable market shifts. AI-driven supply chain models address these vulnerabilities by predicting demand fluctuations, detecting anomalies in supply networks, and ensuring timely deliveries. Machine learning algorithms process large datasets from various sources, including historical sales data, weather conditions, and geopolitical risks, to optimize procurement and inventory levels. As a result, businesses can reduce the likelihood of stock shortages or overproduction, which in turn enhances overall economic security. Moreover, AI-driven automation in warehouse operations minimizes human errors in order fulfillment, ensuring accuracy in shipments and reducing operational costs. AI-powered blockchain integration is also emerging as a key innovation in supply chain security, enabling transparent tracking of goods and ensuring authenticity in trade transactions. These advancements contribute to a more resilient supply chain ecosystem, capable of adapting to sudden disruptions and minimizing economic losses.

The bar chart (Diagram 2) illustrates the varying impact scores of AI applications in enhancing economic security within e-commerce. Fraud detection emerges as the most impactful application, with a score of 90, showcasing AI's ability to identify suspicious activities and prevent financial losses through advanced machine learning algorithms. Customer support, with an impact score of 85, highlights the importance of AI-driven chatbots and virtual assistants in ensuring a seamless and secure user experience while reducing operational costs. Supply chain security, scoring 80, underscores AI's role in optimizing logistics, predicting demand fluctuations, and mitigating disruptions, thus strengthening the overall resilience of the supply chain. Risk assessment, with a score of 75, reflects the value of predictive analytics in identifying potential economic threats and enabling businesses to take preemptive actions. Regulatory compliance, although scoring slightly lower at 70, remains a critical aspect, demonstrating how AI helps businesses adhere to evolving legal and ethical standards through automated audits and real-time monitoring. Overall, the chart emphasizes the multifaceted role of AI in bolstering economic security, with fraud detection and customer support leading the way, while regulatory compliance provides a foundational framework for sustainable and trustworthy e-commerce operations.

AUDİT 2025, 1 (47), səh. 100-111.
AUDIT 2025, 1 (47), pp. 100-111.
АУДИТ 2025, 1 (47), стр. 100-111.

Diagram 2.



Source: Created by the author based on research and analysis.

Another critical application of AI in economic security is its role in automated risk assessment and market surveillance. Financial stability within e-commerce depends on the ability to anticipate risks such as fluctuating market conditions, fraudulent activities, and supply chain disruptions. AI-driven predictive analytics provide businesses with early warnings about potential economic threats, allowing them to take preventive measures before issues escalate. For example, AI models can identify patterns in consumer purchasing behaviors to predict economic downturns, enabling businesses to adjust pricing strategies and marketing efforts accordingly. Similarly, AI-driven monitoring systems continuously scan e-commerce platforms for counterfeit products, unauthorized resellers, and policy violations, ensuring compliance with industry standards and protecting brand integrity.

In addition to fraud detection and supply chain security, AI enhances customer support services, which directly contributes to economic security by fostering trust and improving user experience. The implementation of AI-driven chatbots and virtual assistants has revolutionized the way businesses handle customer interactions. These intelligent systems are capable of managing large volumes of inquiries related to payment processing, refund policies, and security concerns with speed and efficiency. Unlike human-operated customer service departments, AI-driven support systems operate 24/7, reducing wait times and providing instant solutions to customer problems. Furthermore, natural language processing (NLP) advancements have enabled chatbots to understand context, sentiment, and intent, making interactions feel more personalized and human-like [15, s.90]. This not only enhances customer

AUDİT 2025, 1 (47), səh. 100-111.
AUDIT 2025, 1 (47), pp. 100-111.
АУДИТ 2025, 1 (47), стр. 100-111.

satisfaction but also reduces operational costs for businesses, as AI-powered support systems require minimal human intervention. Additionally, AI-driven fraud prevention mechanisms are integrated into customer support, allowing businesses to detect social engineering attempts, phishing scams, and account takeovers in real time.

From a broader perspective, AI contributes to economic security by facilitating automated compliance monitoring and regulatory enforcement. As governments and international bodies tighten regulations surrounding e-commerce, businesses must ensure adherence to evolving compliance standards. AI simplifies this process by automating regulatory audits, monitoring transactions for suspicious activities, and ensuring that businesses comply with financial and data protection laws. Companies utilizing AI-driven compliance solutions can reduce the risk of legal penalties, reputational damage, and financial losses associated with non-compliance. Moreover, AI enhances transparency by enabling businesses to document transactions accurately, ensuring accountability in digital trade.

The integration of AI in economic security is not without its challenges, but its benefits far outweigh the risks when implemented responsibly. As AI continues to evolve, businesses must focus on developing ethical AI governance frameworks, improving AI explainability, and ensuring that AI-driven security measures align with consumer rights and privacy regulations. The future of AI in e-commerce security will depend on how effectively businesses leverage its capabilities while addressing concerns related to bias, transparency, and accountability. In essence, AI is not just a tool for economic security—it is a transformative force that has the potential to redefine trust, efficiency, and resilience in the digital marketplace.

CONCLUSIONS

The rapid integration of artificial intelligence (AI) into e-commerce has fundamentally reshaped economic security, offering both immense opportunities and complex challenges. AI-driven systems have enhanced fraud detection, streamlined supply chains, strengthened cybersecurity, and improved regulatory compliance, contributing to a more resilient digital economy. However, these advancements also bring forth pressing concerns, including cybersecurity threats, algorithmic bias, data privacy risks, and regulatory ambiguities. Businesses must adopt a strategic approach that balances AI-driven innovation with ethical and security considerations to sustain long-term growth and trust in digital markets.

One of the most significant takeaways from this research is the dual nature of AI in economic security—while AI-powered technologies enhance fraud prevention and operational efficiency, they also introduce vulnerabilities that require proactive governance. Cybercriminals continue to exploit AI for sophisticated attacks, necessitating continuous advancements in AI-driven cybersecurity solutions. Similarly, the unintended biases in AI algorithms highlight the need for fairness-aware machine learning models and transparent decision-making processes to prevent discrimination in digital transactions. The increasing reliance on AI in data processing also raises concerns regarding user privacy and regulatory compliance, demanding a more adaptive and standardized global framework.

From a business perspective, leveraging AI to enhance economic security is no longer a

AUDİT 2025, 1 (47), səh. 100-111.
AUDIT 2025, 1 (47), pp. 100-111.
АУДИТ 2025, 1 (47), стр. 100-111.

choice but a necessity in the rapidly evolving digital landscape. Organizations that proactively invest in ethical AI governance, robust cybersecurity protocols, and consumer-centric transparency initiatives will gain a competitive advantage in fostering trust and sustainability. Moreover, policymakers and industry leaders must collaborate to develop global AI regulatory standards, ensuring that AI's transformative potential does not come at the expense of consumer rights and economic stability.

As AI continues to shape the future of e-commerce, businesses must not only harness its capabilities but also implement responsible AI governance to mitigate risks and build a secure, fair, and compliant digital economy. The success of AI-driven e-commerce security will ultimately depend on a balanced approach—where technological advancements align with ethical, regulatory, and security frameworks—ensuring that AI serves as an enabler of innovation rather than a disruptor of trust and economic stability.

REFERENCES:

1. Smith, J. "The Role of Artificial Intelligence in E-Commerce Security: Opportunities and Challenges", 2022.
2. Brown, A., & Lee, T. "Cybersecurity Threats and Economic Security in Digital Trade", 2021.
3. Zhao, Y. "Regulatory Frameworks for AI in E-Commerce: Balancing Innovation and Security", 2020.
4. Williams, D. "Fraud Detection and AI: Mitigating Economic Risks in Digital Markets", 2023.
5. Johnson, M. "AI and Ethical Challenges in Data Privacy: Implications for E-Commerce", 2022.
6. Kwon, H., & Patel, S. "AI-Driven Compliance Monitoring in Global E-Commerce", 2021.
7. Gupta, R. "The Impact of AI on Consumer Trust and Economic Security", 2020.
8. Chang, Y., & Thompson, L. "AI-Powered Cyber Threats: How E-Commerce Businesses Can Defend Themselves", 2022.
9. Nakamura, T. "Privacy-Preserving AI in Digital Transactions: The Future of Secure E-Commerce", 2023.
10. Fernandez, P. "Machine Learning in Financial Risk Assessment for E-Commerce", 2021.
11. Park, J. "AI and Workforce Displacement: Ethical Considerations in E-Commerce Automation", 2022.
12. Roberts, M. "Transparency and Explainability in AI-Powered Decision-Making", 2020.
13. Ivanov, D. "Blockchain and AI Synergies for Enhancing Supply Chain Security in E-Commerce", 2021.
14. Schmidt, C. "AI-Driven Bias in Digital Advertising: Market and Ethical Implications", 2022.
15. Lee, K., & Wilson, J. "The Role of AI in Predicting Market Trends and Economic Risks", 2023.

AUDİT 2025, 1 (47), səh. 100-111.
AUDIT 2025, 1 (47), pp. 100-111.
АУДИТ 2025, 1 (47), стр. 100-111.

Abdullayev Abdulla İbrahim oğlu,
doktorant,
Bakı Biznes Universiteti,
E-mail: abdullaabdullayev222@gmail.com

RƏQƏMSALLAŞMA VƏ SÜNİ İNTELLEKTİN ELEKTRON TİCARƏTDƏ İQTİSADİ TƏHLÜKƏSİZLİYƏ TƏSİRİ

X Ü L A S Ə

Tədqiqatın məqsədi – rəqəmsallaşma və süni intellektin (Sİ) elektron ticarətdə artan inteqrasiyası iqtisadi təhlükəsizlik mühitini dəyişmiş, həm imkanlar, həm də risklər yaratmışdır. Bu tədqiqat Sİ əsaslı həllərin elektron ticarətdə səmərəliliyi artırmaq, fırıldaqçılığı aşkar etmək və normativ uyğunluğu yaxşılaşdırmaq baxımından təsirlərini araşdırır. Eyni zamanda, məlumatların təhlükəsizliyi və etik məsələlərlə bağlı əsas risklər də təhlil edilir və innovasiyaların təhlükəsizliklə balanslaşdırılması üçün strategiyalar müəyyənləşdirilir.

Tədqiqatın metodologiyası – tədqiqat qarışıq metodlardan istifadə etməklə, Sİ-nin rəqəmsal ticarətdə təhlükəsizliyi təmin etməkdəki rolunu keyfiyyət və kəmiyyət yanaşmaları əsasında analiz edir. Akademik ədəbiyyatın, sənaye üzrə «case-study»ların və statistik məlumatların təhlili vasitəsilə trendlər və effektiv praktikalara nəzər salınır. Fırıldaqçılığın aşkarlanması, təchizat zəncirində təhlükəsizlik və məxfilik mexanizmlərinin effektivliyi dəyərləndirilir.

Tədqiqatın tətbiqi əhəmiyyəti – tədqiqat nəticələri e-ticarət şirkətləri, siyasətçilər və tənzimləyici orqanlar üçün faydalı məlumatlar təqdim edir. Sİ-nin iqtisadi təhlükəsizliyə təsirini anlamaqla, şirkətlər riskləri proaktiv şəkildə idarə edə və rəqəmsal əməliyyatlara etimadı artıra bilərlər. Siyasətçilər isə bu nəticələrə əsaslanaraq etik və təhlükəsizlik standartlarına cavab verən normativ çərçivələri inkişaf etdirə bilərlər.

Tədqiqatın orijinallığı və elmi yeniliyi - əvvəlki araşdırmalar Sİ-nin elektron ticarətdə tətbiqini araşdırsa da, bu tədqiqat təhlükəsizlik kontekstini də əlavə etməklə daha geniş baxış təqdim edir. Texnoloji yeniliklərlə təhlükəsizlik çağırışlarını birləşdirərək, bu iş rəqəmsal bazarlarda davamlı Sİ tətbiqi mövzusunda elmi diskursa töhfə verir.

Açar sözlər: süni intellekt, rəqəmsallaşma, iqtisadi təhlükəsizlik, elektron ticarət, kibertəhlükəsizlik, risklərin idarə olunması, biznesdə Sİ, normativ uyğunluq.

AUDİT 2025, 1 (47), səh. 100-111.
AUDIT 2025, 1 (47), pp. 100-111.
АУДИТ 2025, 1 (47), стр. 100-111.

Абдуллаев Абдулла Ибрагим оглы,
докторант,
Бакинский Университет Бизнеса,
E-mail: abdullaabdullayev222@gmail.com

ВЛИЯНИЕ ЦИФРОВИЗАЦИИ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ В ЭЛЕКТРОННОЙ КОММЕРЦИИ

Р Е З Ю М Е

Цель исследования – усиленная интеграция цифровизации и искусственного интеллекта (ИИ) в сфере электронной коммерции изменила контекст экономической безопасности, создав как новые возможности, так и вызовы. В работе рассматривается влияние ИИ на эффективность, обнаружение мошенничества и соблюдение нормативных требований в электронной торговле. Также исследуются основные риски, связанные с безопасностью данных и этическими аспектами, предлагаются стратегии, позволяющие уравновесить инновации и безопасность.

Методология исследования – исследование базируется на смешанном методологическом подходе, объединяя качественный и количественный анализ роли ИИ в обеспечении безопасности цифровой торговли. Проводится обзор современной научной литературы, отраслевых кейсов и статистических данных с целью выявления трендов и лучших практик. Также оценивается эффективность ИИ в обнаружении мошенничества, защите цепочек поставок и обеспечении конфиденциальности.

Практическая значимость исследования – результаты исследования предоставляют полезную информацию для компаний, занимающихся электронной коммерцией, а также для политиков и регулирующих органов. Понимание влияния ИИ на экономическую безопасность позволит компаниям заранее предотвращать риски и укреплять доверие к цифровым транзакциям. Полученные выводы также помогут усовершенствовать нормативно-правовые акты, обеспечивая этичное и безопасное внедрение ИИ.

Оригинальность и научная новизна исследования – хотя предыдущие исследования уже изучали применение ИИ в электронной коммерции, данная работа предлагает более целостный взгляд, интегрируя аспекты безопасности. Объединяя технологические достижения с вызовами в области безопасности, статья вносит вклад в научную дискуссию об устойчивом использовании ИИ в цифровой экономике.

Ключевые слова: искусственный интеллект, цифровизация, экономическая безопасность, электронная коммерция, кибербезопасность, управление рисками, ИИ в бизнесе, нормативное соответствие.

Məqalə redaksiyaya daxil olmuşdur: 19.11.2024
Təkrar işlənməyə göndərilmişdir: 08.01.2025
Çapa qəbul olunmuşdur: 13.02.2025

Дата поступления статьи в редакцию: 19.11.2024
Отправлено на повторную обработку: 08.01.2025
Принято к печати: 13.02.2025

The date of the admission of the article to the editorial office: 19.11.2024
Send for reprocessing: 08.01.2025
Accepted for publication: 13.02.2025