ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 07,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

ARTIFICIAL INTELLIGENCE AND INFORMATION SECURITY: THREATS, APPROACHES AND PROSPECTS IN THE CONTEXT OF MODERN MASS MEDIA

Jartibaeva Biybisara Kuwanishbay qizi
Master's student, Karakalpak State University
Phone: +998 90 263 32 10
Email: biybisarajartbaeva@gmail.com

Annotation: This academic article analyzes the impact of artificial intelligence technologies on information security in the context of contemporary mass media. Based on the June 3, 2025 article published in Yangi O'zbekiston newspaper, the paper evaluates how technological consciousness is shaped in society, the balance between risks and opportunities posed by AI, and how these issues are presented through the media. The article discusses international approaches, legal and ethical challenges of AI, the threat of disinformation, and the use of algorithmic tools to strengthen information security. The experience and strategies of Uzbekistan are examined within a global perspective.
Keywords: artificial intelligence, information security, disinformation, generative AI, mass media, technological consciousness, ethical issues, Yangi O'zbekiston newspaper, fake content, media analysis

The rapid advancement of information and communication technologies (ICT) in recent decades has catalyzed the seamless integration of artificial intelligence (AI) systems into nearly every domain of human activity, including industry, education, healthcare, finance, governance, and media [1]. Initially conceived as a technical means of replicating certain cognitive tasks traditionally performed by humans—such as pattern recognition, problem-solving, and decision-making—AI has since matured into a complex, adaptive system capable of learning, generating content, and interacting in human-like ways [2].

This evolution has expanded the role of AI far beyond narrow, domain-specific applications. Today, AI technologies play a significant role in managing the flow of digital information, shaping public opinion through personalized content delivery, and even influencing high-level decision-making in political and economic spheres [6]. The pervasive use of AI in sensitive areas involving communication, data control, and behavioral prediction has raised critical concerns regarding its impact on information security.

Consequently, AI is increasingly viewed not only as a powerful driver of technological progress and innovation but also as a source of new, complex threats—particularly in relation to privacy, misinformation, and digital manipulation. This dual perspective positions AI as both a valuable asset and a potential risk, necessitating a more nuanced, interdisciplinary approach to its analysis and regulation [1].

This dual nature of artificial intelligence—offering both transformative potential and serious risks—has made it a central topic of discussion not only within academic and technological communities but also across mass media platforms. Among recent media contributions, the article titled "Artificial Intelligence: A Threat to Information Security or a Key to Progress?", published in the June 3, 2025 edition of Yangi O'zbekiston, stands out as a significant and timely intervention. It plays a notable role in shaping public perception by presenting a balanced analysis of AI's promises and perils, thereby encouraging deeper societal engagement with the topic [5].

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 07,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

In order to thoroughly assess the impact of artificial intelligence on information security, it is essential to first examine how AI technologies operate, the domains in which they are applied, and the broader social mechanisms they interact with. Early AI systems were largely confined to rule-based expert models that relied on predefined logic and structured data. However, modern AI systems have evolved significantly, now incorporating sophisticated techniques such as deep learning, generative adversarial networks (GANs), and natural language processing (NLP), which allow machines to process unstructured information, learn from vast datasets, and produce outputs that closely mimic human cognition [2].

Among these advancements, the rise of generative AI has introduced particularly complex challenges. Tools powered by generative models are capable of creating hyper-realistic synthetic content, including text, images, audio, and video. One of the most notable—and alarming—developments in this area is the proliferation of deepfake technologies, which enable the creation of fabricated media that can convincingly imitate real individuals and events [2]. Such content, while technologically impressive, poses serious threats to the integrity of information. It can be used to spread misinformation, manipulate public opinion, incite social unrest, and even damage diplomatic relations between countries when weaponized in geopolitical contexts [7]. These risks underscore the urgent need for robust detection systems, legal frameworks, and public awareness strategies to mitigate the harmful effects of such misuse.

At the same time, cyber threats powered by artificial intelligence have grown significantly in scale and complexity. Malicious actors now use AI to carry out automated phishing attacks, manipulate online discourse through bot-driven campaigns, and create fake social media profiles designed to influence public opinion or polarize communities [6]. These practices illustrate how AI technologies are increasingly being weaponized—not merely as tools for efficiency or data processing, but as mechanisms for strategic influence and psychological operations in digital environments. In such scenarios, AI transcends its technical utility and takes on ideological, political, and even geopolitical dimensions [4].

In this regard, the article published in Yangi O‘zbekiston offers substantial value by presenting a nuanced examination of both the promises and the perils of AI. It highlights AI as an “artificial alternative to human thinking,” a phrase that encapsulates the transformative scope of the technology while also signaling the need for caution and critical oversight [5]. By promoting a balanced societal outlook, the article fosters thoughtful engagement with AI rather than blind enthusiasm or fear. From a scholarly perspective, this equilibrium—acknowledging both opportunities and risks—is vital for maintaining objectivity and methodological rigor in the study of emerging technologies [1].

Globally, many legislative frameworks have been introduced to regulate AI’s impact on security. The European Union's “Artificial Intelligence Act” categorizes AI systems by risk level and outlines specific regulatory strategies for each [3]. In the United States, the “AI Bill of Rights” proposes ways to protect human rights in the age of AI [4]. These documents provide insight into how global powers aim to manage the societal consequences of AI.

In Uzbekistan, the recent adoption of strategic documents such as the “AI Development Concept” and the “Digital Technology Development Strategy – 2030” highlights AI as a driver of national development [7]. However, these policies give insufficient attention to the issues of information security and personal data protection [6].

AI can also be used to enhance information security. For example, advanced cybersecurity systems now rely on AI to detect anomalies, analyze user behavior, predict threats, and make

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 07,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

real-time decisions [7]. Furthermore, AI algorithms are capable of identifying fake content, filtering misinformation, and blocking malicious materials [1]. However, such technologies raise questions of personal privacy, surveillance, and ethical boundaries. AI-powered monitoring systems may restrict personal freedoms if unchecked [4]. Thus, any technological solution must be harmonized with legal and ethical standards.

How AI is portrayed in mass media plays a crucial role in shaping public perception and societal acceptance. The article published in Yangi O‘zbekiston addresses this responsibility with depth and balance, taking a thoughtful approach to the social, philosophical, and ethical dimensions of artificial intelligence. It not only presents technological advancements but also critically examines the risks and challenges associated with them, thereby encouraging public awareness and informed discourse. Particularly noteworthy is the article’s philosophical reflection on the evolving relationship between humans and technology, which contributes to preventing common misconceptions and fostering a more nuanced understanding of AI’s role in society [5].

In academic practice, analyzing such journalistic materials proves to be highly beneficial. These sources serve not only as reflections of public discourse but also as active contributors to shaping technological literacy and societal attitudes toward innovation. By contextualizing complex topics like artificial intelligence in accessible language, they help bridge the gap between scientific communities and the general public. Moreover, media narratives influence how societies interpret technological change and can significantly shape public policy priorities and regulatory approaches [6][7].

In conclusion, artificial intelligence is an essential technological force in modern society, closely connected to information security. It offers great potential for development, such as improving cybersecurity and managing data efficiently. However, without proper regulation and ethical oversight, it can pose serious threats — including disinformation, privacy violations, and social manipulation.

Therefore, AI must be studied and managed from scientific, legal, and societal perspectives to ensure it supports human progress rather than undermines it. Mass media plays a crucial role in this process by informing the public and encouraging thoughtful debate. The article published in Yangi O‘zbekiston represents a positive example of such responsible engagement. Efforts like this are important for building public awareness and guiding AI development in a balanced, secure, and ethical direction.

References:

1. Floridi, L. (2021). The Ethics of Artificial Intelligence. Oxford University Press.
2. Bostrom, N. (2014). Superintelligence: Paths, Dangers, Strategies. Oxford University Press.
3. European Commission. (2021). Artificial Intelligence Act – Proposal for a Regulation.
4. The White House. (2022). Blueprint for an AI Bill of Rights. https://www.whitehouse.gov
5. “Sun’iy intellekt: Axborot xavfsizligiga tahdidmi yoki taraqqiyot kaliti?” – Yangi O‘zbekiston, June 3, 2025, Issue No. 111.
6. Qodirov A., Karimov S. (2022). “Sun’iy intellektning huquqiy asoslari: xalqaro va milliy tajriba.” Yuridik fanlar jurnali, №2, pp. 45–56.
7. Uzinfocom. (2023). O‘zbekistonda raqamli xavfsizlik strategiyalari va AI texnologiyalari. Official report.