JOURNAL OF MULTIDISCIPLINARY SCIENCES AND INNOVATIONS
VOLUME 5, ISSUE 03
MONTHLY JOURNALS
ISSN NUMBER: 2751-4390
IMPACT FACTOR: 9,08

ARTIFICIAL INTELLIGENCE AND INFORMATION SECURITY PROBLEMS

Babayev Sirojiddin Saidkamolovich
Programming teacher, Urgench branch, KhorezmregionTeacher,
Asia International University

Abstract

This article examines the role and significance of artificial intelligence in modern society, as well as the information security challenges associated with its use. It highlights the capabilities of artificial intelligence in rapid data analysis, workflow automation, and improving efficiency across various fields. The concept of information security and its core principles—confidentiality, integrity, and availability—are briefly explained. Special attention is given to the analysis of deepfake technologies and fake content generated with the help of artificial intelligence, along with their negative impact on information reliability, fraud, and the spread of misinformation. In conclusion, the article emphasizes the importance of verifying information, relying on trustworthy sources, and following security measures when using artificial intelligence technologies.

Keywords

Artificial intelligence, information security, deepfake, fake content, confidentiality, information reliability.

Аннотация

В статье рассматриваются роль и значение искусственного интеллекта в современном обществе, а также связанные с его применением проблемы информационной безопасности. Освещаются возможности искусственного интеллекта в области быстрого анализа данных, автоматизации рабочих процессов и повышения эффективности в различных сферах деятельности. Кратко раскрывается сущность информационной безопасности и её базовые принципы: конфиденциальность, целостность и доступность. Особое внимание уделяется анализу deepfake-технологий и фальшивого контента, создаваемого с использованием искусственного интеллекта, а также их негативному влиянию на достоверность информации, распространение мошенничества и дезинформации. В заключение подчеркивается необходимость проверки информации, использования надежных источников и соблюдения мер безопасности при работе с технологиями искусственного интеллекта.

Introduction

Nowadays, artificial intelligence (AI) technologies are rapidly developing and are increasingly being integrated into various areas of society. In particular, the use of artificial intelligence in education, healthcare, finance, industry, and information services plays an important role in accelerating work processes, analyzing data, and improving efficiency. At the same time, the widespread application of AI technologies is also creating new challenges related to information security.

The Importance of Artificial Intelligence

Artificial intelligence plays an important role today in the development of society and technology. Its main significance lies in the rapid analysis of large volumes of data, reducing human labor, and automating work processes. With the help of artificial intelligence, complex tasks can be completed faster and more accurately.

In addition, artificial intelligence increases efficiency in many fields such as education, healthcare, banking, industry, and transportation. For example, in healthcare, it helps diagnose diseases, while in education, it provides personalized recommendations for students. As a result, time is saved, service quality improves, and the decision-making process becomes simpler.

In the future, the role of artificial intelligence will continue to grow. Therefore, it is important to use it correctly, safely, and responsibly.

The Concept of Information Security

Information security is the process of protecting data from unauthorized access, theft, modification, deletion, or distribution. In other words, it means keeping information secure and ensuring that only authorized persons can use it.

The main goals of information security are:

- maintaining confidentiality (so that unauthorized people cannot see it),
- ensuring integrity (so that the data is not altered),
- maintaining availability (so that it can be accessed when needed).

For example, setting a password on your phone, enabling a verification code for your Telegram account, and installing antivirus software on your computer — all of these are part of information security.

Deepfakes and Fake Content

A deepfake is fake video, audio, or image content that is created or modified using artificial intelligence. For example, it is possible to place a person's face into another video or create fake audio that imitates their voice. Such content can look very similar to real material on the surface.

Fake content, on the other hand, refers to false or misleading information that can spread in the form of text, images, audio, or video. Since artificial intelligence can help create such content quickly and on a large scale, it poses a serious problem for information security.

CONCLUSION

In conclusion, artificial intelligence plays an important role in modern society, creating great opportunities to improve work efficiency, rapidly analyze data, and automate processes in various fields. At the same time, its widespread use is increasing a number of information security problems, including the spread of deepfakes and fake content.

Ensuring information security today is not only a technical issue but also a social one. Detecting false information, using trustworthy sources, and improving users' information literacy play an important role in reducing these problems.

References

1. Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.

2. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
3. National Institute of Standards and Technology (NIST). (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce.
4. National Institute of Standards and Technology (NIST). (2004). Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199). U.S. Department of Commerce.
5. International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2022). ISO/IEC