MIDI 2024 Conference

Large Language Models Vulnerabilities Criticality: IMECA-based Analysis of Attacks and Countermeasures

Abstract

Large Language Models (LLM) have a positive impact on many areas of society, but the security of systems that integrate and use these models is at risk. In addition to widespread public attention, LLM-based systems (LLMS) are also attracting attention from cybercriminals. Given these factors, assessing the vulnerabilities of LLMS and improving their security is an important task that is addressed in this article. The main vulnerabilities of LLMS are considered and classified. The criticality of these vulnerabilities is analyzed in accordance with the provisions of the Intrusion Modes Effects Criticality Analysis (IMECA) method. The matrices of criticality of LLM cyber risks before and after the use of countermeasures are built and it is determined which of the vulnerabilities change the level of criticality. The directions for future research on developing a model for collecting and analyzing LLM vulnerabilities that cause a high level of cyber risks to the system and do not have significant countermeasures for protection are substantiated.