

KInIT in Quark magazine: When an AI agent crosses the line

Datum 6.10.2026
Subjekt Kempelenov inštitút inteligentných technológií
Region Slovensko
Kategorie Technologie, Věda a výzkum, Bezpečnost

Our collaboration with Quark magazine continues with another article in the series focused on intelligent technologies. Quark is a Slovak popular science magazine dedicated to science and technology, where you can find KInIT's contributions in both print and online formats.

In the October issue, our Technology Lead Martin Tamajka explores the cybersecurity risks associated with AI agents. His article, *When an AI Agent Crosses the Line: What Three Security Incidents Reveal*, looks at what can happen when these systems take actions their developers did not anticipate.

Martin explains how AI agents differ from language models and chatbots, and how they use tools to carry out tasks across multiple steps. The more tools and permissions a system receives, the wider the range of actions it can take, increasing both its capabilities and the potential for things to go wrong.

The article also explores why the language we use to describe AI matters. Talking about these systems as if they had human intentions can complicate questions of responsibility. As Martin explains, carrying out steps autonomously does not mean independently setting goals.

You'll find the full article in the October issue of Quark. Subscribers can also read it online.

<https://kinit.sk/kinit-in-quark-magazine-when-an-ai-agent-crosses-the-line>