Dirbtiniu intelektu grįsti sprendimai kibernetinei saugai gerinti

Prof. dr. Igoris Belovas, doc. dr. Rasa Brūzgienė, doc. dr. Agnė Brilingaitė, prof. dr. Linas Bukauskas, doc. dr. Kęstutis Driaunys, prof. dr. Olga Kurasova, doc. dr. Viktor Medvedev, doc. dr. Vytautas Evaldas Rudžionis

Didėjant šiuolaikinių technologijų sudėtingumui ir nuolat augančiam kibernetinių grėsmių mastui, dirbtinio intelekto taikymas tampa svarbia kibernetinio saugumo stiprinimo priemone. Mašininis mokymasis, gilusis mokymasis ir kitos dirbtiniu intelektu grįstos technologijos leidžia kurti inovatyvius sprendimus, skirtus anomalijoms ir kenkėjiškai programinei įrangai aptikti, identifikuoti grėsmes realiuoju laiku, tobulinti autentifikavimo sprendimus ir kurti proaktyvius prevencinius gynybos mechanizmus. Todėl pagrindinis šios temos tikslas – kurti inovatyvius teorinius ir praktinius sprendimus, kurie užtikrintų didesnį skaitmeninių sistemų atsparumą ir patikimumą nuolat kintančioje kibernetinėje aplinkoje.

Artificial intelligence-based solutions to improve cybersecurity

As modern technologies become increasingly complex and the scale of cyber threats continues to expand, the application of artificial intelligence (AI) has become a critical tool for enhancing cybersecurity. Machine learning, deep learning, and other AI-driven technologies enable the development of innovative solutions for detecting anomalies and malware, identifying threats in real-time, improving authentication methods, and creating proactive defense mechanisms. Therefore, the primary objective of this research topic is to develop innovative theoretical and practical solutions that ensure greater resilience and reliability of digital systems in an ever-changing cyber threat landscape.