Перспективы развития и защиты систем с применением ИИ-агентов

Список использованных источников

1. Применение искусственного интеллекта на финансовом рынке: текущий статус и условия дальнейшего развития, доступен по адресу https://www.cbr.ru/Content/Document/File/185193/Consultation_Paper_20112025.pdf
2. Искусственный интеллект в нефтегазовой отрасли, отчет экспертной группы форума TNF2025 https://oilgasforum.ru/mail/TNF2025_web.pdf
3. The controllability trap: a governance framework for military ai agents https://arxiv.org/abs/2603.03515
4. Регуляторные документы РФ по безопасности ИИ — с чем мы вступаем в 2026 год https://habr.com/ru/articles/986800/
5. О рисках применения искусственного интеллекта при защите КИИ https://bisa.ru/stati/o-riskakh-primeneniya-iskusstvennogo-intellekta-pri-zaschite-kii
6. Safety by Desing — новая Clean Architecture. И как же ее достичь?

   https://habr.com/ru/articles/987980/
7. The zero-days are numbered https://blog.mozilla.org/en/privacy-security/ai-security-zero-day-vulnerabilities
8. OpenClaw-RL: Train Any Agent Simply by Talking https://arxiv.org/pdf/2603.10165