

Karim Karimov

MSc Candidate, Science, Technology and Innovation Management and Policy

✉ mirakky99@gmail.com 📍 Campinas, São Paulo, Brazil

🌐 <https://mirakky.com> 🐙 github.com/mirakky 📌 t.me/mirakky

Research Interests

AI security and the safety of machine learning systems; adversarial robustness and ML-based threat detection; the governance and policy dimensions of securing AI infrastructure. My work sits at the intersection of applied security engineering and technology policy – I am interested in how technical safeguards for AI systems can be designed so that they are actually enforceable in practice.

Education

University of Campinas (UNICAMP)

Master

Business Administration

Campinas, São Paulo, Brazil • Aug 2026 – expected 2027

Dual-degree exchange program with NRU HSE.

Master's thesis: *From Reactive to Proactive Cybersecurity: The Role of Generative AI and Large Language Models in Predictive Threat Management* • Advisor: Izabela S. Rampasso

National Research University "Higher School of Economics"

Master

Science, Technology and Innovation Management and Policy

Moscow, Russia • Sep 2025 – expected 2027

National Research University "Higher School of Economics"

Bachelor

Information Security

Moscow, Russia • Sep 2021 – Jul 2025

Publications

Public Perception of Innovation – Good for Society or Made by the Devil?

Aug 2026

The Social Life of Innovation, HSE Basic Research Program Working Papers, WP BRP 130/STI/2026, pp. 70–75

Chapter in an edited collection with contributors from HSE, Tsinghua, BUPT and UNICAMP.

<https://doi.org/10.2139/ssrn.7275238>

Research Experience

AI Pentest Tool – LLM-Assisted Vulnerability Triage

Apr 2026 – Present

Independent project

- Built a tool orchestrating seven open-source scanners and using a locally hosted LLM to correlate their output into a single CVSS-scored report mapped to OWASP Top 10 and MITRE ATT&CK.
- Designed the analysis layer to run entirely on-device, so scan data never leaves the operator's machine – a constraint that rules out hosted models for security-sensitive assessments.

<https://github.com/mirakky/ai-pentest>

Research Assistant / QA Engineer – MLOps Execution and Monitoring System for AI Models

Jan 2025 – May 2025

HSE MIEM (Moscow Institute of Electronics and Mathematics), Moscow

• Designed and implemented automated testing for the internal APIs and web interfaces of an MLOps platform used to deploy and monitor production ML models; built test coverage for model-serving endpoints, catching integration failures before deployment.

Research Practicum: Deep Learning for Web Attack Detection Jan 2023 – Mar 2023
HSE MIEM, Moscow

• Reproduced a CNN-BiLSTM intrusion detection architecture and evaluated it on web-attack classification over CIC-IDS2017 network flow data using stratified 5-fold cross-validation.

• Benchmarked it against a Random Forest baseline, which outperformed the deep model on recall and F1; the network failed almost entirely on the minority XSS and SQL-injection classes.

<https://github.com/mirakky/web-attack-detection-cnn-bilstm>

Teaching and Curriculum Development

Methodologist-Analyst and Frontend Developer – Administration of Systems and Networks
Nov 2024 – May 2025
HSE MIEM, Moscow

• Authored more than 20 laboratory and practical assignments from scratch for an undergraduate systems and networks course; designed and implemented the web interface of the course delivery platform.

Work Experience

Sberbank-Service (technology subsidiary of Sberbank, Russia's largest bank) Moscow
Software Engineer Jun 2023 – Jul 2026

• Built automated test suites (TypeScript, Jest, Appium) across web, mobile and API layers for five production products.

• Designed load-testing scenarios for backend and AI inference platforms using Locust and Python, identifying bottlenecks prior to release.

• Integrated automated testing into GitLab CI; used Grafana and the ELK stack for observability and failure analysis.

Technical Skills

Programming Languages TypeScript, Python, C++, SQL

ML and Security Network intrusion detection, Cryptographic implementation, Applied ML

Infrastructure Docker, GitLab CI, PostgreSQL, Grafana, ELK

Testing Jest, Appium, Locust, REST API testing

Languages

Russian	English	Portuguese	German
Native	C1; TOEFL scheduled Oct 2026	A2	A2
●●●●●	●●●●○	●●○○○	●●○○○