

Grigoriy Zaitsev

AI Security Engineer · Saint Petersburg · 21

Email: dev@suspectus.ru
Telegram: @zkprooff
Site: suspectuso.ru/en

Languages: English B2 · Chinese HSK 3 · Russian (native)

Education

- **SUAI (GUAP), Saint Petersburg**: BSc in Information Security, 3rd year. Labs on AI security; building a secure LLM deployment in university practice — *09.2024 — 06.2028*
- **Sirius × Alfa-Bank**: «AI Technology Security» (MLSecOps) — *05 — 06.2026*
- **NSU Summer School on Cryptography**: research track, co-author of a paper — *07.2025*
- **PROJECTOR 10.0**: project and innovation lab — *2025*

Experience

- **«Sdaete»** — *Saint Petersburg*
  Application Security · P2P rental marketplace — *03.2026 — 06.2026*

  OWASP ASVS L2 | TypeScript | NestJS | PostgreSQL | Docker

  ◦ Three rounds of security review before due diligence: 43 vulnerabilities found and fixed, including XSS, IDOR, PII leaks, rate-limit bypass and non-idempotent webhooks.

  ◦ Added AES-256-GCM for PII, refresh-token rotation, RBAC, HMAC and idempotency keys for payments.

Selected Projects

- **Sirius Argus: secure MLOps platform (Alfa-Bank × Sirius, MLSecOps)**

  Team of 4 | FastAPI | MLflow | Keycloak | ART | Docker

  ◦ Proposed the Zero Trust architecture and access model. Model control pipeline: code, dependency and artifact scans, model signing, CI security gates, adversarial tests with ART, runtime drift detection. Coverage of OWASP ML Top 10, MITRE ATLAS, NIST AI RMF.
- **ML security selection case (Sirius × Alfa-Bank), 3rd of 110**

  PyTorch | PGD | Model extraction | Backdoor detection

  ◦ Targeted adversarial attack with PGD, model extraction with fidelity 1.0, backdoor detection with IoU 1.0.
- **GIGAPROTO: multi-agent LLM orchestrator (Prosto × Sber × ITMO hackathon)**

  Python | FastAPI | GigaChat | pgvector

  ◦ Pipeline of parser, analyst, designer, validator, refiner and recommender agents that turns a requirements document into a validated mobile UI schema.
- **Self-hosted AI infrastructure**

  GPU server | Local open-weight LLMs | GitLab | Prometheus | Grafana

  ◦ Own server with a local LLM lab, GitLab, monitoring and alerting.

Achievements

Top 3, Sirius × Alfa-Bank «AI Technology Security»: 3rd of 110 in selection — *05.2026*
Winner, Sber Business × Future Leaders Foundation case championship: 1st of 25 teams — *2025*
2nd place, AI BUSINESS SPb Hackathon, Mediascope case — *2026*
6th of 23 teams, TON Winter Mini Hackathon, 2nd in the audience vote — *2025*
Hackathons, Prosto × Sber × ITMO (GIGAPROTO) · Changellenge CUP IT × OTP (HQA 25%) · CUP Russia × VTB — *2024–26*
Programs, City Volunteers Leadership School (team lead) · Future Leaders Foundation: top 30 of 2000+ · Soft Skills Lab · PROJECTOR 10.0 — *2023–26*
CTF, T-CTF · AlfaCTF ×2 · organised SUAI CTF at my university — *2025–26*
Volunteering, «Professionals 2024»: best volunteer · Missing-person search (EMERCOM) · First aid (Red Cross) — *2023–26*

Publications

- **Zero-knowledge proof protocol in smart contracts.** *SummerCrypto 2025, NSU, pp. 250–258.* zk-SNARK with ZoKrates and a Solidity verifier for Ethereum, Merkle tree membership.
- **From attacking models to securing their lifecycle (MLSecOps).** *Case write-up, 2026.* Adversarial attacks, model extraction, backdoor detection.
- **Sirius Argus: secure MLOps platform.** *Project write-up, 2026.* Architecture and security controls.

Programming Skills

Languages:	Python, Go, TypeScript, SQL, Bash
Frameworks & Tools:	PyTorch, ART, MLflow, Ollama, RAG, FastAPI, Keycloak, Docker, Kubernetes, GitLab CI, Prometheus, Grafana, Loki; MITRE ATLAS, OWASP LLM Top 10, NIST AI RMF.