

Vladimir Evgrafov

Engineering leadership, systems architecture, and LLM-agent security

[vovapi.ru](#)[LinkedIn](#)[GitHub](#)[Google Scholar](#)

EXPERIENCE

Viasat Tech - Chief Technology Officer

February 2025 - present | Moscow | viju streaming service

- Lead development, QA, infrastructure, architecture, and the AI track across a 35-person technology department.
- Raised quarterly plan completion from 40% to 83%; teams shipped about 100 releases across seven platforms in 2025.
- Cut Android crash rate 14x to 0.17%, halved video start time, and launched a new product stream on all platforms simultaneously.

Viasat Tech - Head of Software Development

January 2022 - February 2025 | Moscow

- Joined as the technology department's second hire, recruited 35 engineers, QA specialists, and analysts, and established delivery processes.
- Designed and implemented a Go microservice backend that sustains 100x the load at one quarter of the resource consumption.

Atlas Biomed - Backend Team Lead

April 2020 - January 2022 | healthtech

- Built a multi-service system for processing and interpreting medical data.

TRMPLN Media - Golang Developer

October 2018 - April 2020 | adtech

- Developed a high-load, fault-tolerant ad-serving system with safe handling of personal data.

Multy - Golang Developer

March 2018 - October 2018 | fintech

- Built microservices that integrated with financial systems.

Okmeter - Golang Developer

September 2017 - December 2017 | monitoring

- Worked on agents that collected metrics from Linux devices and processes.

SolidWall - Python Developer

July 2015 - June 2017 | application security

- Maintained the Python codebase, software build and deployment system, CI, and monitoring.

PROFILE

I am the CTO of the viju streaming service. I lead a 35-person technology department across seven web, mobile, TV, backend, and systems-analysis teams.

I am a hands-on engineering leader who grew from Go development into department leadership. I built an engineering organization from scratch, migrated legacy systems to microservices, and own architecture, infrastructure, budget, and AI.

SELECTED IMPACT

35

people in the department

7

teams and platforms

100x

supported-load increase

14x

Android crash-rate reduction

CORE EXPERTISE

- Engineering leadership
- Systems architecture
- Go and microservices
- DevOps and reliability
- ML and recommendations
- LLM agents and AI security

EDUCATION

PhD candidate - Artificial Intelligence

Lomonosov Moscow State University, CMC | expected 2027

Thesis on security for LLM-based agentic systems: attack methods and defenses for autonomous agents.

MSc - Artificial Intelligence

Lomonosov Moscow State University, CMC | 2021

Developed a method for converting conventional neural networks into spiking networks while preserving accuracy and improving inference efficiency.

BSc - Applied Mathematics and Computer Science

Lomonosov Moscow State University, CMC | 2019

Built grammar-oriented fuzzing for web-template engines to uncover XSS, server-side code execution, and denial-of-service defects.

RESEARCH

I research the security of autonomous LLM systems: prompt injection, attacks on memory, tools and protocols, multimodal threats, and inference-time defenses.

SELECTED PUBLICATIONS

2026

Auditing Inference-Time Defense Evaluation for Multimodal Large Language Models

arXiv, cs.CR

2026

Attack Methods and Defenses in LLM-Based Agentic Systems

International Journal of Open Information Technologies 14 (5)

2023

A Review of Potential Risks of Systems with Multimodal Language Models

Tikhonov Readings

2021

Spiking Neural Networks

International Journal of Open Information Technologies 9 (7)

TECHNICAL FOCUS

- Go
- Python
- Microservices
- Distributed systems
- Cloud / DevOps
- Observability
- Recommender systems
- LLM systems

RESEARCH INTERESTS

- LLM agent security
- Inference-time defenses
- Multimodal models
- AI evaluation
- Spiking neural networks

ENGAGEMENT

Open to part-time or project engagements as a fractional CTO, technical advisor, or consultant on architecture and AI platforms.

PROFILES

- vovapi.ru
- LinkedIn
- GitHub
- Google Scholar