

Владимир Евграфов

Engineering leadership, архитектура и безопасность LLM-агентов

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

ОПЫТ РАБОТЫ

viju - Технический директор (СТО)

Январь 2022 - настоящее время | Москва | streaming

- Нанял 35 инженеров, тестировщиков и аналитиков; выстроил 7 продуктовых и платформенных команд.
- Спроектировал и внедрил микросервисный backend на Go: система выдерживает нагрузку в 100 раз выше при четырехкратном снижении потребления ресурсов.
- Поднял выполнение квартальных планов с 40% до 83%; за 2025 год команды выпустили около 100 релизов на 7 платформах.
- Снизил Android crash rate в 14 раз, до 0,17%; вдвое сократил время старта видео и запустил новый продуктовый стрим на всех платформах.

Atlas Biomed - Backend Team Lead

Апрель 2020 - январь 2022 | healthtech

- Разрабатывал систему из множества сервисов для обработки и интерпретации медицинских данных.

TRMPLN Media - Golang Developer

Октябрь 2018 - апрель 2020 | adtech

- Разрабатывал высоконагруженную отказоустойчивую систему показа рекламы и безопасную обработку персональных данных.

Multy - Golang Developer

Март 2018 - октябрь 2018 | fintech

- Разрабатывал микросервисы для интеграции с финансовыми системами.

Okmeter - Golang Developer

Сентябрь 2017 - декабрь 2017 | monitoring

- Участвовал в разработке сервиса мониторинга Linux-устройств и процессов.

SolidWall - Python Developer

Июль 2015 - июнь 2017 | application security

- Развивал Python-кодovou базу, систему сборки и внедрения ПО, CI и мониторинг.

ПРОФИЛЬ

Я технический директор viju. Руководжу технологическим департаментом из 35 человек и семью командами. Мы развиваем стриминговый сервис для веба, мобильных устройств и TV-платформ.

Я СТО с техническими корнями: вырос из Go-разработчика, построил департамент с нуля и перевел legacy на микросервисы. Отвечаю за архитектуру, инфраструктуру, бюджет и AI-направление.

КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ

35

человек в департаменте

7

команд и платформ

100x

рост поддерживаемой нагрузки

14x

снижение crash rate Android

КОМПЕТЕНЦИИ

- Engineering leadership
- Архитектура систем
- Go и микросервисы
- DevOps и надежность
- ML и рекомендации
- LLM-агенты и AI security

ОБРАЗОВАНИЕ

Аспирантура - искусственный интеллект

МГУ имени М.В. Ломоносова, ВМК | защита ожидается в 2027

Диссертация о безопасности агентных систем на базе больших языковых моделей: атаки на LLM-агентов и методы защиты.

Магистратура - искусственный интеллект

МГУ имени М.В. Ломоносова, ВМК | 2021

Метод преобразования классических нейронных сетей в спайковые: сохранение точности при более энергоэффективном событийном выводе.

Бакалавриат - прикладная математика и информатика

МГУ имени М.В. Ломоносова, ВМК | 2019

Грамматико-ориентированный фаззинг шаблонизаторов веб-страниц для поиска XSS, серверного выполнения кода и отказов в обслуживании.

ИССЛЕДОВАНИЯ

Исследую безопасность автономных LLM-систем: prompt injection, атаки на память, инструменты и протоколы, мультимодальные угрозы и методы защиты во время инференса.

ИЗБРАННЫЕ ПУБЛИКАЦИИ

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

Обзор возможных рисков использования систем с мультимодальными языковыми моделями

Тихоновские чтения

2021

Спайковые нейронные сети

International Journal of Open Information Technologies 9 (7)

ТЕХНИЧЕСКИЙ ФОКУС

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

НАУЧНЫЕ ИНТЕРЕСЫ

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

ФОРМАТ РАБОТЫ

Открыт к частичной занятости и проектной работе как fractional CTO, технический советник или консультант по архитектуре и AI-платформам.

ПРОФИЛИ

[vovapi.ru](#)

[LinkedIn](#)

[GitHub](#)

[Google Scholar](#)